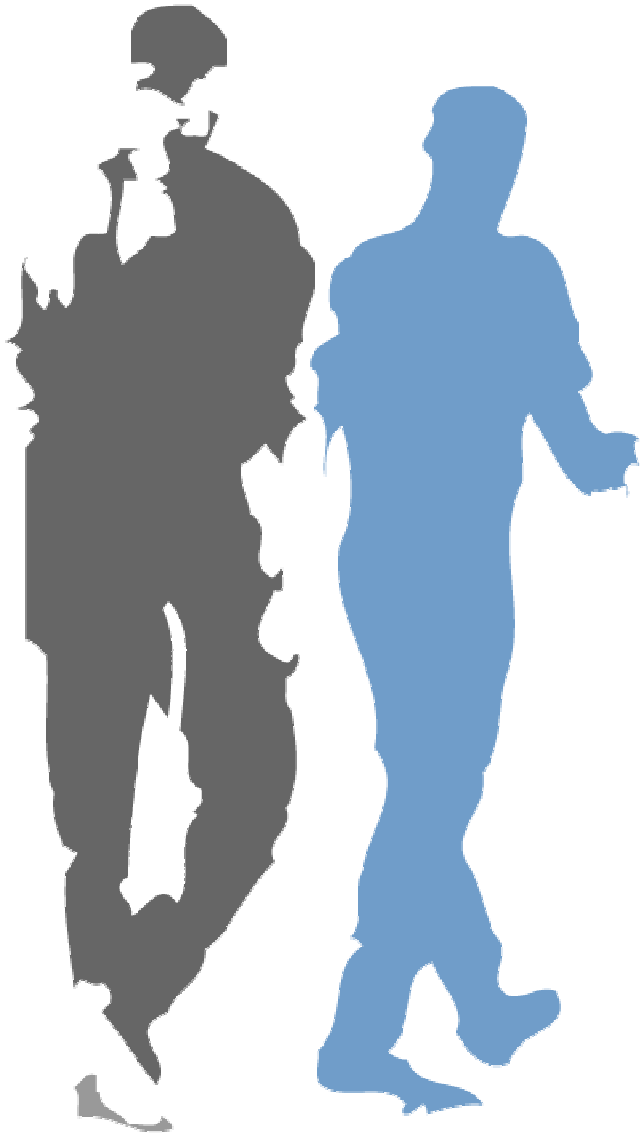
milestone

XProtect

Transact 2.5

Administrator's Manual



milestone

Target Audience for this Document

This document is intended for system administrators. This document explains how to install and configure Milestone XProtect Transact as an add-on to a Milestone XProtect surveillance system.

Descriptions about how to browse transaction data and video recordings together using the *Viewer* or the *Smart Client* are available in the Milestone XProtect Transact User's manual aimed at end users who solely use Transact for browsing transaction data and video recordings.

Copyright, Trademarks and Disclaimer

Copyright

© 2007 Milestone Systems A/S.

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This help system is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in this help system's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

Contents

INTRODUCTION 7

PRODUCT OVERVIEW 7

INTERACTION WITH SOURCES AND SURVEILLANCE SOLUTIONS 8

SYSTEM REQUIREMENTS 9

Transact Server 9

Client (Viewer or Smart Client with plugin) 9

INSTALLATION AND LICENSING 10

INSTALLING THE SOFTWARE 10

UPDATING FROM A PREVIOUS VERSION 13

ABOUT LICENSING 14

REGISTERING YOUR SOFTWARE LICENSE CODE (SLC) 14

OBTAINING ADDITIONAL LICENSES 17

GETTING STARTED 18

ADMINISTRATION 19

MANAGING SERVER SETTINGS 19

SOURCES AND CONFIGURATIONS 20

Different Source Providers 21

Reader-friendly Data through Configurations 21

Advanced Event Features 22

MANAGING SOURCES 22

Adding a New Source 22

Editing a Source 23

Deleting a Source 23

Suspending/Resuming a Source 23

Refreshing the Status of Sources 24

The Create/Edit Source Window's Dialog Elements 24

MANAGING CONFIGURATIONS 27

Creating a Configuration 27

How to Capture Transaction Data 31

Editing a Configuration 32

Copying a Configuration 32

Exporting/Importing a Configuration 33

How to Omit Characters 34

How to Use Substitutions 34

How to Add Line Breaks 35

How to Use Start and Stop Masks 35

The Create/Edit Configuration Window 36

The Edit Filter Window 38

The Select Input Source Window 39

MASTER/SLAVE SETUP 39

Managing Master/Slave Setup 40

EVENTS AND EVENT GROUPS 41

Managing Events 42

Managing Event Groups 44

How to Create a Generic Event Triggered by Transaction Data 45

How to Test Events 47

Viewing Alerts Triggered by Transaction Events in the Smart Client ... 49

Viewing Alerts Triggered by Transaction Events in Viewer 50

STORAGE AND LICENSING SETTINGS 50

CLIENT-SIDE PREPARATIONS 52

INTEGRATING WITH MILESTONE XPROTECT CORPORATE 52

INSTALLING THE TRANSACT PLUGIN FOR THE SMART CLIENT 55

CREATING A VIEW WITH TRANSACTIONS IN THE SMART CLIENT 59

REMOVING THE SOFTWARE 62

REMOVING THE TRANSACT SOFTWARE 62

REMOVING THE DATABASE 62

REMOVING THE TRANSACT PLUGIN INSTALLER 62

REMOVING THE SMART CLIENT PLUGIN 63

USING THE BUILT-IN HELP SYSTEM 64

NAVIGATING THE BUILT-IN HELP SYSTEM 64

THREE TYPES OF LINKS IN HELP TOPICS 65

PRINTING HELP TOPICS 65

GLOSSARY 66

Introduction

Product Overview

Milestone XProtect Transact is a powerful tool for tracking transactions linked with video recordings of the transactions taking place.

Milestone XProtect Transact is an add-on to Milestone's IP video surveillance solutions XProtect Basis+, XProtect Professional, XProtect Enterprise and XProtect Corporate. Milestone XProtect Transact can combine your digital video monitoring with transaction data from many kinds of transaction data sources and for many purposes. You get a 1-to-1 correspondence of images to transactions and the transaction data is time-linked with simultaneous display of transactions and camera recordings.

Common transaction data sources are PoS (Point of Sale) or ATM (Automatic Teller Machine) which enables you to easy investigate and prove fraud. But actually any transaction data source that you would like to time-link with digital video monitoring can be combined through Milestone XProtect Transact. A few examples of other transaction data sources and purposes are: number plate recognition for collection of road taxes, access control for combined visual identification for higher security—but the only limit is your imagination. Note, that some solutions might require additional programs and/or customizations.

The examples used in this manual show typical retail situations and transactions data from PoS (Point of Sale) or ATM (Automatic Teller Machine). For these purposes Milestone XProtect Transact speeds up investigations into fraud by integrating digital video surveillance images with PoS (Point of Sale) or ATM (Automatic Teller Machine) transaction data: 1-to-1 correspondence of images to transactions. Transaction data is time-linked with video images of cash registers/ATMs for simultaneous display of transactions and camera recordings. Whether the problem is internal or external perpetrators, it is easy to find suspicious transactions with Milestone XProtect Transact's features for searching transactions by cash register/ATM, camera, data, time or free text. See Viewing Transactions on page 52 for more information.

See Interaction with Sources and Surveillance Solutions on page 8 for more information about how Transact interacts with the sources and your surveillance solution.

Interaction with Sources and Surveillance Solutions

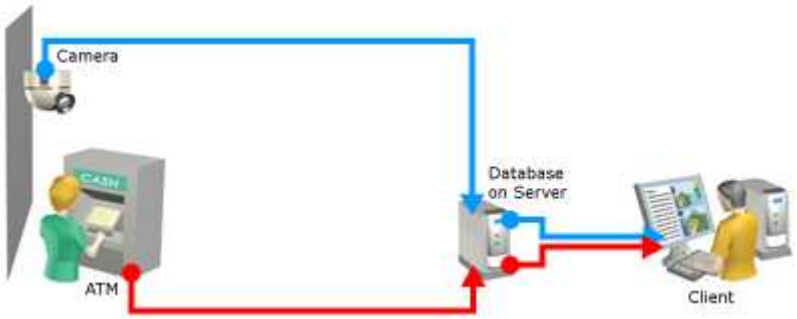
There are several players in the Transact communication flow.

In short, Milestone XProtect Transact consists of a Transact Server and a Transact Database.

The Transact Server has a service that listens for transactions from *sources*. Four different kinds of source exist: Serial ports, TCP clients, TCP XML and Troy boxes (more types may be available in customized Transact installations). Sources, in turn, are connected to the actual devices on which the transaction data is generated (cash registers, ATMs, etc.).

When the Transact Server receives transaction data from a source, it stores the data in the Transact Database.

Video recordings are stored independently on your surveillance server, as defined through the configuration of your XProtect surveillance solution.



Example only: The blue arrows outline video recordings from the surveillance system, while the red arrows outline transaction data from sources.
In addition to an ATM, transaction data may also come from a cash register or any other RS-232-enabled device.

System Requirements

The following are minimum system requirements for using Milestone XProtect Transact:

Transact Server

CPU: Intel® Pentium® 4 or compatible, minimum 2.4 GHz.

RAM: 512 MB.

Network: Ethernet (100 Mbit recommended).

Operating System: Microsoft® Windows® XP Professional, Microsoft Windows Server 2003 or Windows Vista™.

Software: Microsoft .NET 3.0 framework required. Milestone XProtect Corporate 1.5 or newer or Milestone XProtect Enterprise 6.0 or newer or Milestone XProtect Professional 6.0 or newer or Milestone XProtect Basis+ 6.0 or newer required. Milestone XProtect Smart Client 3.0 or newer required.

Client (Viewer or Smart Client with plugin)

CPU: Intel Pentium 4 or compatible, minimum 2.4 GHz.

RAM: 512 MB.

Network: Ethernet (100 Mbit recommended).

Graphics Card: AGP or PCI-Express, 1024×768.

Operating System: Microsoft Windows XP Professional, Microsoft Windows Server 2003 or Windows Vista.

Software: Microsoft .NET 3.0 Framework required.

Installation and Licensing

Installing the Software

Note: Read the License Terms on the Product License Sheet (enclosed with the software CD) before installing Milestone XProtect Transact.

IMPORTANT: If you are updating from a previous version of Milestone XProtect Transact, read Updating from a Previous Version on page 13 before removing the old Transact version.

Prerequisites: Before installing the software, register your Transact Software License Code (SLC). When the license is registered, a Connection License Key (CLK) is generated. You need the CLK during the installation. See Registering Your Software License Code (SLC) on page 14 for more information. Check whether you have the latest version of Microsoft .NET Framework 3.0. You can download .NET Framework 3.0 from Microsoft's Download Center at www.milestonesys.com/downloads.

Note: If you are installing Milestone XProtect Transact on a computer running Windows Vista, you must run the installation as an administrator.

Note: Install Transact on the same computer as the server for Milestone XProtect Enterprise Milestone XProtect Professional or Milestone XProtect Basis+ or on the same computer as the management server for Milestone XProtect Corporate.

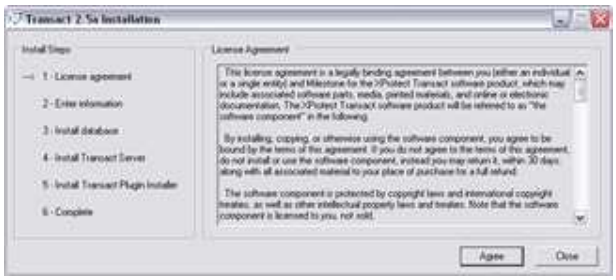
To install Milestone XProtect Transact, do the following:

1. Insert the Milestone XProtect Transact software CD

   On the CD, double-click the file *TransactInstaller.exe*.

   If installing a version downloaded from the internet, simply run the .exe file from the location at which you have saved it.

   After a short wait, the *Transact Installation* window will open:

   Read the license agreement, then click the *Agree* button to accept the license terms and go to the next step.

2. In the *Software License Code (SLC)* field, type the Software License Code for your Milestone XProtect Transact solution.

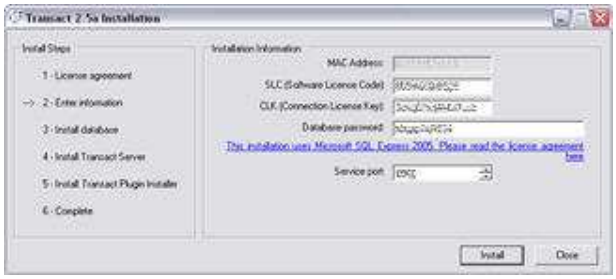
   Tip: The Software License Code is printed on the Product License Sheet enclosed with the Milestone XProtect Transact software CD.

   In the *Connection License Key (CLK)* field, type the CLK (Connection License Key) that was

generated when you registered your Software License Code (SLC).

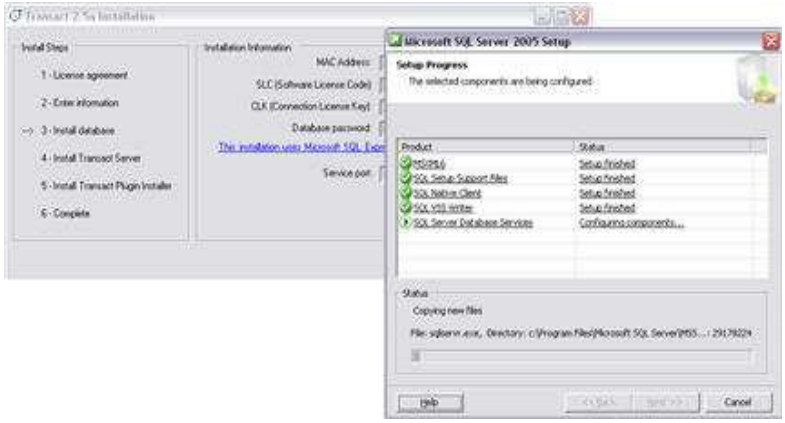
In the *Database password* field either simply use the default database password *temppwd124* or type a new password of your own choice.

Read the license agreement for Microsoft SQL Express 2005 by clicking the *This installation uses Microsoft SQL Express 2005. Please read the license agreement here.* link.



When ready, click the *Install* button.

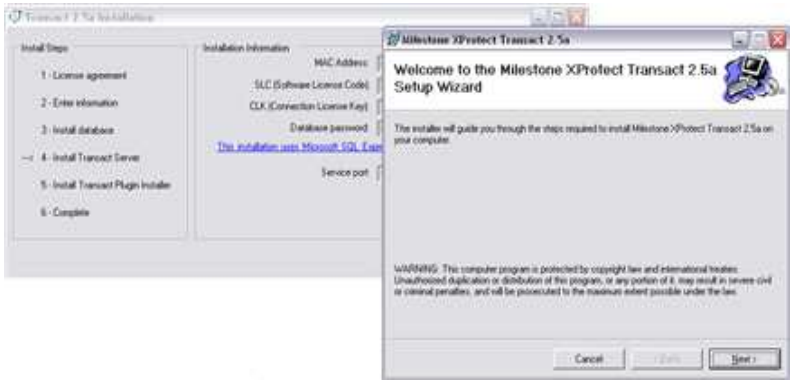
3. On the third installation step, the Microsoft SQL Server 2005 Express Edition used for handling the Transact database will be installed:



If you are updating from a previous version of Milestone XProtect Transact, you will be asked if you would like to install Microsoft SQL Server 2005 Express Edition which is Transact's new database, or update the database of the previous version. We recommend you install the new database application. See Updating from a Previous Version on page 13 for more information.

The installation may take a short while, after which you are automatically taken to the fourth installation step.

4. On the fourth installation step, Milestone XProtect Transact (the Transact Server, Transact Services and Transact Administrator) will be installed. A wizard opens:



In the wizard, click *Next* to continue.

Type your name in the *Name* field, and the name of your organization in the *Organization* field, then click *Next*.

Select required installation folder (a default installation folder is automatically suggested). Also select whether just yourself or anyone using the computer should be able to access Milestone XProtect Transact (if in doubt, select *Everyone*). Then click *Next*.

Click *Next* again to start the actual installation of the Transact Server.

When Transact Server installation is complete, click *Close* to return to the main installation window.

5. On the fifth installation step, the Transact Plugin Installer will be installed.

   The Plugin Installer is a utility which will enable Smart Client users to download a plugin from the Transact Server; the plugin will allow them to view transaction data in their Smart Clients.

   A wizard opens. In the wizard, click *Next* to continue.

   Select required installation folder (a default installation folder is automatically suggested). Also select whether just yourself or anyone using the computer should be able to access the Transact Plugin Installer (if in doubt, select *Everyone*). Then click *Next*.

   Click *Next* again to start the actual installation of the Transact Plugin Installer.

   When installation of the Transact Plugin Installer is complete, click *Close* to return to the main installation window. The fifth installation step is not applicable for your version of Transact; installation will automatically move to step 6.

6. The Milestone XProtect Transact installation is complete. Click *Close* to exit the installation window.

   You are now able to open the *Transact Administrator* window, in which you configure your Milestone XProtect Transact solution: You access the *Transact Administrator* window by double-clicking the *Transact Administrator* desktop shortcut. Alternatively, you can access it from Windows' *Start* menu, by selecting *Start > All Programs > Milestone Transact > Transact Administrator*.

7. To view transaction data in the Smart Client you need to install the Transact plugin for the Smart Client.

- **With Milestone XProtect Enterprise Milestone XProtect Professional or XProtect Basis+**
  To enable the Smart Clients to time-link transactions from Transact with video recordings from a Milestone XProtect Enterprise Milestone XProtect Professional or XProtect Basis+ solution, do the following:
  Open an Internet Explorer browser (version 6.0 or later), and connect to *http://localhost:[portnumber]/* on the computer with the Transact Plugin Installer. Replace *[portnumber]* with the port number used by your Milestone IP video surveillance solution. The port number is defined in the *Image Server* application.

  To enable end-users to view transaction data in the Smart Client, you must send them information about the URL or IP address of the computer with the Transact Plugin Installer and the Image Server's port number (*http:///[URLorIP]:[Portnumber]/*).

- **With Milestone XProtect Corporate**
  To enable the Smart Clients to time-link transactions from Transact with video recordings from a Milestone XProtect Corporate solution, do the following:

  Locate TransactPluginInstaller.exe on the computer with the Transact installation (typically in C:\Program Files\Milestone\Milestone XProtect Transact Smart Client Plug-in Installer 2.5). Copy the file to the computer with the relevant Smart Clients installation and doubleclick the exe file. Follow the instructions on the screen.

  To enable end-users to view transaction data in the Smart Client, you must make the TransactPluginInstaller.exe file available to them, for instance by placing a copy of the file on your network.

See Installing the Transact Plugin for the Smart Client on page 55 for more information.

Updating from a Previous Version

If you are updating from a previous version of Milestone XProtect Transact, note the following:

- Prior to installing Transact 2.5, you must remove the Transact software, Transact Plugin Installer and any Smart Client Plugins of the previous Transact version.

- Milestone XProtect Transact 2.5 uses a new database (Microsoft SQL Server 2005 Express Edition) compared to previous versions of Transact (Microsoft SQL Server Desktop Engine).

- Transact 2.5 can use the old database, but we recommend installing the new—and better—Transact 2.5 database.

  If a previous Transact database is detected on the computer during the installation, you will be asked whether you want to install the new database Microsoft SQL Server 2005 Express Edition, or update the old database.

  If you choose to install the new database, the old database and its content are moved to a new folder but remain on the computer and new transaction data will be stored in the new database. However, Transact 2.5 cannot read data from the old database or make it available for browsing or viewing.

  If you have much data that is important for you to keep, update the old database. If you have less data for instance seven days of transaction data, export the data from the old database with the export features in the Smart Client before you remove the previous Transact installation and install Transact 2.5 with the new database.

Note: Even if the old database and its content remain on the computer, if you choose to install the new database, it is not possible for you to access the data in the old database by removing Transact 2.5 and reinstalling Transact 2.2. If it is very important for you to access the old database, you can contact your Milestone vendor.

For information about the export features in the Smart Client see Exporting Data and Recordings in the Smart Client in the Milestone XProtect Transact User's manual and the separate documentation for the Smart Client.

About Licensing

When you purchase Milestone XProtect Transact, you also purchase two types of licenses:

- **Software License Code (SLC):** A license to use the Milestone XProtect Transact application.
- **Connection License Key (CLK):** A license for a certain number of simultaneously opened transaction sources.

During the installation you are asked to enter both the SLC and the CLK. The Software License Code is printed on the Product License Sheet enclosed with the Milestone XProtect Transact software as well as on your order confirmation. You must, however, register your SLC to get the CLK. See Registering Your Software License Code (SLC) on page 14 for more information.

You can add an unlimited number of transaction sources in Milestone XProtect Transact. See Managing Sources on page 22 for more information. You can, however, only view the number of simultaneous transaction sources corresponding to your CLK. You can at any time obtain a new CLK with more simultaneously viewed transaction sources. See Obtaining Additional Licenses on page 17 for more information.

Registering Your Software License Code (SLC)

When you purchase Milestone XProtect Transact software you receive a Software License Code (SLC). The SLC is printed on the product license sheet enclosed with the software CD as well as on your order confirmation.

You should register your SLC before installing Milestone XProtect Transact, since you also need a Connection License Key (CLK) during the installation. Note, that a CLK is called a DLK on the registration website. See About Licensing on page 14 for more information about the two types of licenses.

The registration process is brief and easy. To register your SLC, do the following:

1. Go to the Milestone Systems website at www.milestonesys.com, and click the *Software registration* link in the menu:

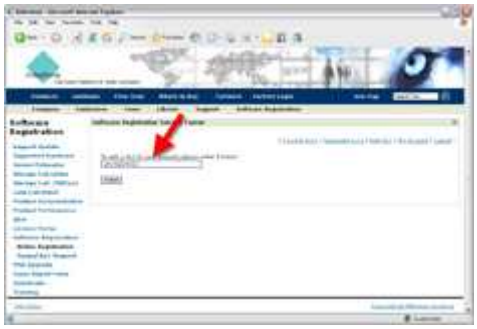
Illustrations are examples only; website layout may change over time

2. Log in to the Software Registration Service Center with your user name (e-mail address) and password.

   Tip: If you have not used the Software Registration Service Center before, click the *New to the system?* link, and follow the instructions for registering yourself as a user; then log in to the Software Registration Service Center using your registered user name and password.

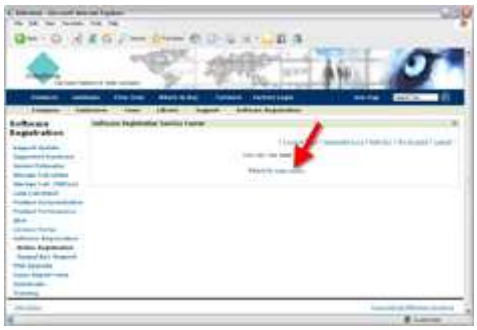
3. In the Software Registration Service Center, click the *Add SLC* link:

4. Type your SLC and click *Submit*:



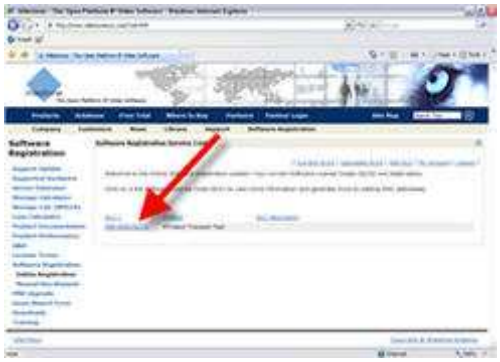
   When asked whether you want to add the SLC to your account, click *OK*.

5. Once your SLC has been added, click the *main menu* link:



6. You are now ready to obtain a Connection License Key (CLK) – a license for the number of sources you can view.

   Click the link representing your Transact SLC:



7. Click the *Add new MAC* link to register the MAC address of the computer on which you are installing the Milestone XProtect Transact software.

   Tip: A MAC address is a 12-digit hexadecimal number (example: 0123456789AF), also called the computer's Physical Address. To find the computer's MAC address do the following: Click *Start* -> *Run*. Type *cmd* in the *Open* field and click *OK*. Write *ipconfig /all* on the command prompt. Find the Physical Address. When you write the MAC address omit all hyphens: The MAC address 01-23-45-67-89-AF must be written as 0123456789AF during the registration.

8. Type the computer's MAC address in the first field.

9. Then type a description in the second field (for example the computer's IP address, physical location or user). Such descriptions will help you quickly recognize each computer, especially helpful if you have several installations of XProtect Transact.

10. Click the *Submit* button.

11. When asked whether you want to add the device's MAC address to the SLC, click OK.

12. Click the *Get all keys via email* link to have your CLK sent to you by e-mail.

13. Click the *Logout* link to log out of the Software Registration Service Center.

Obtaining Additional Licenses

If you want to view more simultaneous transaction sources than you currently have licenses for, you must purchase additional licenses for these transaction sources. You can add and configure an unlimited number of transaction sources in Milestone XProtect Transact, but only simultaneously view the number of sources that are included your CLK.

To obtain additional licenses for your XProtect Transact system, contact your XProtect Transact vendor.

Once you have obtained the required additional licenses, do the following to activate them:

1. When you have received a confirmation about the purchase of the new licenses, go to the Milestone Systems website at www.milestonesys.com, and click the *Software registration link in the menu.*

   Log in to the *Software Registration Service Center* with your user name (e-mail address) and password.

   Click the link representing your Transact SLC.

2. Copy the updated CLK's 16-digit hexadecimal number displayed on the page.

3. Start the Transact Administrator, and click the *General Settings* tab.

4. In the *Connection License Key (CLK)* field, replace the current CLK by pasting the updated CLK into the field.

5. If relevant, click the *Sources* tab, select an existing suspended source and click the *Resume* button to be able to view data from this source. You can also add new sources. See Managing Sources on page 22 for more information.

6. Click *Close* to exit the Transact Administrator.

Getting Started

Once the Transact Server is installed, it is recommended that you perform configuration tasks in the following order:

1. Verify that transaction data will be stored in the Transact Database for sufficiently long to cover your organization's needs.

   By default, transaction data will be stored for seven days, but you are able to change this default value on the *Transact Administrator* window's *General settings* tab.

   Note that when defining individual sources (see next step), you are furthermore able to define individual transaction data storage lengths for each source.

2. Add your Transact's sources. A source is a data source, typically a serial server, through which transaction data is fed to the Transact Server and subsequently stored in the Transact Database. See Managing Sources on page 22 for more information.

   As part of defining a source, you define a configuration for the source. A configuration handles the transformation of received data into presentable data. This is necessary because the initially received data typically consists of a single string of information, in which it can be difficult to see when individual transactions begin and end. If the data originates from a printer connection, it may furthermore contain non-printing control characters used for indicating line breaks, etc. By using configurations, the received data can be presented to end-users in a format matching real-life receipts. You are of course able to base your configurations on real transaction data sampled from your sources. See Creating a Configuration on page 27 for more information.

   Tip: Transact comes with a built-in configuration called *Epson default*. Epson is a widely recognized printer manufacturer; thus Epson's way of dealing with control characters is often supported by printers from other manufacturers as well. You can often save time by basing your configuration on a copy of the *Epson default* configuration. See Creating a Configuration on page 27 and Copying a Configuration on page 32 for more information.

3. Enable browsing and viewing of transaction data together with video recordings using the Smart Client or Viewer application. See Viewing Transactions on page 52 for more information. Note that the extremely feature-rich Smart Client is available with a Milestone XProtect Enterprise and XProtect Professional and XProtect Corporate surveillance solution only, and that browsing of transaction data in the Smart Client requires a plugin (see Installing the Transact Plugin for the Smart Client on page 55).

Administration

The Transact Server is the service that listens for transactions from cash registers and other sources, and stores such transactions in the Transact Database. End-users can browse recordings and transaction data with the Milestone XProtect solution's *Viewer* or Milestone XProtect *Smart Client*. See Viewing Transactions on page 52 more information.

All administration of settings related to the Transact Server as well as settings related to how data is transferred to and presented in the client applications is handled in the *Transact Administrator* window. The *Transact Administrator* window also lets you determine how long time transaction data is stored. See Getting Started on page 18 for recommended configuration tasks after the installation of Transact.

You access the *Transact Administrator* window by double-clicking the *Transact Administrator* desktop shortcut. Alternatively, you can access it from Windows' *Start* menu, by selecting *Start* > *All Programs* > *Milestone Transact* > *Transact Administrator*.

The *Transact Administrator* window is divided into following tabs: *Server Settings*, *Sources*, *Masters*, *Events*, *Event Groups* and *General Settings*. See Managing Server Settings on page 19, Sources and Configurations on page 20, Master/Slave Setup on page 39, Events and Event Groups on page 41 and Storage and License Settings on page 50 for more information about how to configure the different Transact settings.

Managing Server Settings

On the Transact Administrator window's *Server Settings* tab you can define general server settings for the Transact Server, and the ports and services used for communication between the Transact Server, the Transact Administrator, any Transact master/slave servers and the client applications.

The tab is divided into two sections: *Service setup* and *Service control*.

Detail from *Transact Administrator* window's *Server settings* tab

Service setup

The *Transact Administrator* window's *Service setup* section has the following content:

- ***Service name*:** The Transact server's default name for the service communicating with the Smart Client is *Service*. You can change the name if another application's service has the same name.

- ***Adminstration service name*:** The Transact server's default name for the service communicating with the Transact Administrator is *Admin*. You can change the name if another application's service has the same name.

- ***Host*:** Lets you specify the local IP address or host name of the Transact Server installation.

  Example of a host name: OurDevice
  Example of an IP address: 123.123.123.123

- ***Port*:** Lets you specify the local port number on which communication between the Transact Server, any Transact master/slave servers and the client applications should take place. The default port number is 9001.

  If you want to change the port number, make sure you select a port number which is not already in use for other purposes. Click the *Set* button to begin using the new port number.

  Tip: To verify which ports are in use on a given computer, select *Start* > *All Programs* > *Accessories* > *Command Prompt*. In the command prompt window, type *netstat -a* and press ENTER to display a list of all current TCP/IP network connections and listening ports. For more information about the various parameters to use with the *netstat* command, type *netstat /?* and press ENTER.

- ***Outside host*:** Lets you specify the outside IP address of the Transact Server installation so it can be accessed over the internet.

- ***Outside port*:** Lets you specify the outside port number on which communication between the Transact Server and the client applications should take place so they can communicate over the internet.

Service control

The *Transact Administrator* window's *Service control* section has the following content:

- ***Stop Transact Service*:** Lets you stop the Transact Server service. When the service is stopped, the button changes to *Start Transact Service*, allowing you to quickly start the service again.

  IMPORTANT: As long as the service is stopped, it will not listen for transactions from cash registers or other sources, and will therefore not store such transactions in the Transact Database.

Sources and Configurations

A *sourc*e is a data source through which transaction data is fed to the Transact Server and subsequently stored in the Transact Database. Transaction data can originate from cash registers, ATMs, etc. The connection between the Transact Server and the cash registers, ATMs, etc. is in the Transact Administrator established through the definition of a source provider. For a diagram outlining the role of sources in the Transact communication flow, see Interaction with Sources and Surveillance Solutions on page 8.

The initially received data from sources typically consists of a single long string of information, and includes control characters or other characters that are irrelevant and confusing when end-users want to view the transaction data. You are able to transform the transaction data of this kind into a presentable, reader-friendly form through configurations. Configurations are managed in the Transact Administrator window's *Sources* tab since configurations are associated with and customized to the different sources.

Different Source Providers

There are four different kinds of source providers through which the transaction data is fed from a PoS, ATM or others to the Transact Server:

- *Troy Box Transact provider*: Use when receiving transaction data from a Troy box on your network through port 9100. *Troy box* is a popular name for a Troy serial server. Provided the Troy box has been assigned an IP address, it is able to receive serial input from a cash register, ATM or any other RS-232 source and relay it to the Transact Server through your network.

- *Serial Port Transact provider*: Use when receiving transaction data as input on the computer's own serial port.

- *TCP XML Transact provider*: Use when receiving transaction data through a serial server device and the transaction data is fed as XML packages. It is prerequisite that the content of the XML packages includes a time stamp in the following format: *<Timestamp>date and time according the RFC 3339 standard</Timestamp>*.

- *TCP Client Transact provider*: Use when receiving transaction through any kind of serial server device. This option also allows you to receive data directly from a PoS (Point of Sale) source, such as a cash register, provided the PoS source can be configured for this purpose.

Note: Additional kinds of sources may be available in customized Transact installations.

When creating and editing a source, the different source settings vary depending on your choice of source provider. See Managing Sources on page 22 for more information about how to create or edit sources.

Reader-friendly Data through Configurations

You are able to omit and substitute characters and define where individual transactions begin and end, so end-users can view the transaction data in a format matching real-life till receipts, ATM receipts, etc. If the data originates from a printer connection, it may for instance contain unprintable characters used for indicating line breaks, when to cut off a till receipt, etc.

By creating a configuration, you are able to:

- Clearly define when individual transactions begin and end.
- Make sure line breaks are used as required.
- Filter out unwanted characters.
- Substitute characters, if required.

See How to Omit Characters on page 34, How to Use Substitutions on page 34, How to Add Line Breaks on page 35 and How to Use Start and Stop Masks on page 35 for more information

Tip: Transact comes with two built-in configurations called *Epson default* and *Analytics*. The *Analytics* configuration is only available for sources that use the source provider *TCP XML Transact provider*. *Epson default* is available for all the other source providers. Epson is a widely recognized printer manufacturer; thus Epson's way of dealing with control characters is often supported by printers of other makes as well. You can often save time by basing your configuration on a copy of the *Epson default* configuration. See Copying a Configuration on page 32 for more information.

Note: The built-in configuration for the *TCP XML Transact provider*, *Analytics*, contains the necessary configuration for transaction data received as XML packages through a serial server device. Further configuration is not needed.

Configurations are managed in the Transact Administrator window's *Sources* tab since configurations are associated with and customized to the different sources. See Creating a Configuration on page 27 for more information.

Advanced Event Features

Through Milestone XProtect Transact's event and event group features you are able to get Transact to listen for occurrences of specific words, numbers, characters etc. in the transaction data and generate events when the specified occurrences are found. Sources are also associated to event groups in the Transact Administrator window's *Sources* tab. See Managing Sources on page 22 and Events and Event Groups on page 41 for more information.

Managing Sources

A source, also called a *source provider*, is a data source through which transaction data is fed to the Transact Server and subsequently stored in the Transact Database.

You define and edit the source settings for the Transact Server by clicking the *Sources* tab in the *Transact Administrator* window.

Adding a New Source

To add a source, do the following:

1. Open the *Transact Administrator* window.

   You access the *Transact Administrator* window by double-clicking the *Transact Administrator* desktop shortcut. Alternatively, you can access it from Windows' *Start* menu, by selecting *Start* > *All Programs* > *Milestone Transact* > *TransactAdministrator*.

2. On the *Transact Administrator* window's *Sources* tab, click the *Add New...* button. This will open the *New Source* window.

3. In the *New Source* window, specify a name for the new source in the *Source name* field, and select the required type of source in the *Source providers* list. See Sources and Configurations on page 20 for more information about the available sources providers and their use.

   Tip: If required, the source name may contain spaces and special characters, such as @, $, %, æ, etc.

   Then click *OK* to go to the *Create Source* window, in which you specify properties for the source.

4. Specify the required settings for how long you want to save transaction data, and the different properties for the selected source provider. See The Create/Edit Source Window's Dialog Elements on page 24 for more information about each setting.

5. Select a built-in standard configuration.

   - If you are defining a source that uses the source provider *TCP XML Transact provider*, select the built-in standard configuration *Analytics* from the list in the *Configuration* section.

- For all other source providers select the built-in standard configuration *Epson default* from the list in the *Configuration* section.

You can add a new configuration or edit the built-in standard configuration later. See Creating a Configuration on page 27 and Editing a Configuration on page 32 for more information about how to create a new configuration or edit an existing one.

6. If you have defined transaction events and event groups, you can associate the source with an event group in the *Event Group* list, to trigger actions through generic events defined in the surveillance system. You can add an event group later. See Events and Event Groups on page 41 for more information.

7. When ready, click *OK*.

   The new source will now appear in the *Transaction sources list* on the *Transact Administrator* window's *Sources* tab.

Editing a Source

To edit the properties and configuration of an existing source, do the following:

1. Open the *Transact Administrator* window.

   You access the *Transact Administrator* window by double-clicking the *Transact Administrator* desktop shortcut. Alternatively, you can access it from Windows' *Start* menu, by selecting *Start* > *All Programs* > *Milestone Transact* > *TransactAdministrator*.

2. On the *Transact Administrator* window's *Sources* tab, select the required source and click the *Edit...* button. This will open the *Edit Source* window.

3. Change the required settings for the selected source. See The Create/Edit Source Window's Dialog Elements on page 24 for more information about the sources settings and The Create/Edit Configuration Window on page 36 for more information about the different configuration settings.

   Click *OK* to save the changes.

Deleting a Source

To delete a source, do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Sources* tab, select the required source and click the *Delete...* button.

3. Click *Yes* to confirm the deletion.

Suspending/Resuming a Source

When the source is running, you can click the *Suspend* button to stop the source. Since you only have Connection License Keys to view a certain number of sources simultaneously, this could be a reason for you to stop one source so you can start another. See About Licensing on page 14 for more information.

You can start or stop the connection from a suspended or running source selected in the Transaction sources list. On the *Transact Administrator* window's *Sources* tab you can see whether your sources are running or suspended.

IMPORTANT: While the source is suspended, no transaction data will be fed from the source to the Transact Server and onwards to the client applications.

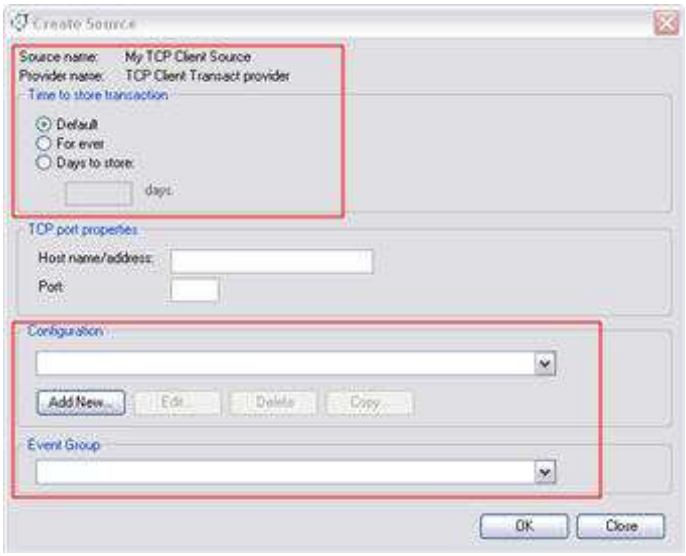
When the source is suspended, the button changes to *Resume*. Clicking the *Resume* button will lift the suspension, and data will again be fed from the source to the Transact Server and onwards to the client applications (provided the Transact Server service is running). See Managing Server Settings on page 19 for more information.

Refreshing the Status of Sources

If a source is unavailable, the source in question will be displayed as *Disabled* on the *Sources* tab. When the source is available again, click the *Refresh* button to refresh the displayed status of the source in *Transact Administrator* window.

The Create/Edit Source Window's Dialog Elements

Much of the content of the *Create/Edit Source* window is the same regardless of which type of source you are creating or editing.



The *Create source* window. Common settings for all sources are highlighted with red rectangular frames.

Source/Provider name

In this information section you can see the name of the source and source provider you are creating:

- ***Source name*:** Read-only field displaying the name of the source as defined in the *New Source* window.
- ***Provider name*:** Read-only field displaying the type of the source as defined in the *New Source* window.

Time to store transaction

The *Time to store transaction* section lets you specify how long transaction data from the source in question should be kept in the Transact Database. The following options are available:

- ***Default*:** Use the Transact solution's default. Transaction data older than the default number of days will be deleted from the Transact Database, and will therefore not be available for browsing in the client applications.

  Tip: The Transact solution's default number of days, i.e. the number of days which transaction data will be stored if nothing else is specified for individual sources, is defined on the *Transact Administrator* window's *General settings* tab. See Storage and License Settings on page 50 for more information.

- ***For ever*:** Store transaction data for ever.

  Note: Even when *For ever* is selected, the ability to store transaction data will be limited by the available disk space on the computer running the Transact Database.

- ***Days to store*:** Lets you specify the required number of days for which to store transaction data for the source in question. The number of days may be higher as well as lower than the Transact solution's default.

  Transaction data older than the specified number of days will be deleted from the Transact Database, and will therefore not be available for browsing in the client applications. Make sure the number of days is sufficiently high to cover your organization's needs.

Configuration

The *Configuration* section lets you manage the source's configuration. See Creating a Configuration on page 27 and Editing a Configuration on page 32 for more information.

- ***[List of existing configurations]*:** Lets you select the configuration to use for the source in question.

  Tip: A single configuration can be used for several transaction data connections as long as the transaction data come from a source of the same type as the source for which the configuration was created.

  By selecting a configuration from the list, you furthermore get access to editing, deleting or copying the selected configuration (see description of the *Edit...*, *Delete* and *Copy...* buttons).

- ***Add New...*:** Opens the *Create Configuration* window, in which you are able to define the properties of a new configuration. See Creating a Configuration on page 27 for more information.

- ***Edit...*:** Available only when an existing configuration is selected.

  Opens the *Edit Configuration* window, in which you are able to edit the properties of the selected configuration.

- ***Delete*:** Available only when an existing configuration is selected.

  Lets you delete the selected configuration. You will be asked to confirm that you want to delete the configuration.

- ***Copy...*:** Available only when an existing configuration is selected.

Lets you copy the selected configuration, edit it as required and save it under a new name. Editing and saving takes place in the *Create Configuration* window.

This may be especially relevant if you require two or more near-identical configurations, in which case you are able to base subsequent configurations on an existing one, thus minimizing your workload.

Event group

The *Event group* section lets you associate the source with an event group. The event group can then trigger actions through generic events defined in Milestone XProtect Enterprise or Milestone XProtect Professional. See Events and Event Groups on page 41 for more information.

Some of the content of the *Create/Edit Source* window is specific for the source you have chosen.

Troy Box Sources

The ***Troy Box properties*** section lets you specify where to contact the Troy box on your network. The following field is available:

- **Host name/address:** Lets you specify host name or IP address of the Troy box.

  Example of a host name: OurDevice
  Example of an IP address: 123.123.123.123

  Tip: You do not need to specify a port number. Transact knows that Troy boxes always communicate through port 9100.

Serial Port Sources

The ***Serial port properties*** section lets you specify settings related to the serial port acting as source. The following fields are available:

- ***COM Port*:** Select the COM port (i.e. serial port) to be used for receiving data from the source.

- ***Bits per second*:** Select the bit rate (i.e. data transfer rate) with which data will be sent on the serial connection.

  Note: The specified bit rate must match the bit rate used by device (cash register, ATM, etc.) connected to the serial port source.

- ***Flow control*:** Select the flow control to be used on the serial connection.

  Flow control adjusts the flow of data from one unit to another, making sure that the receiving unit will be able to handle all the incoming data. The use of flow control is relevant in asynchronous communication, for example when the sending unit sends data faster than the receiving unit is able to receive it.

  - ***None*:** Do not use flow control.

  - ***XonXoff*:** Use the XonXoff flow control mechanism, with which the receiving unit sends an *Xoff* message to the sending unit when the receiving unit's buffer is full. When this is the case, the sending unit will stop sending data until it gets an *Xon* message from the receiving unit, indicating that the receiving unit is again ready to receive data. *Xon* and *Xoff* messages are sent as part of the data itself.

- ***CtsRts*:** Use the CtsRts flow control mechanism, with which the sending unit sends an *Rts* (Ready to send) signal to the receiving unit when the sending unit has data to send. In turn the receiving unit will send a *Cts* (Clear to send) signal to the sending unit when the receiving unit is ready to receive data. *Cts* and *Rts* signals are sent on separate wires in the cable, apart from the data itself.

- ***DsrDtr*:** Use the DsrDtr flow control mechanism, with which units send *Dsr* (Data set ready) and *Dtr* (Data terminal ready) signals when exchanging data.

Note: The selected flow control mechanism must match the flow control mechanism used by device (cash register, ATM, etc.) connected to the serial port source.

TCP XML or TCP Client Sources

The ***TCP port properties*** section lets you specify settings related to the TCP port on which the TCP XML or TCP client provider will be acting as source. The following fields are available:

- ***Host name/address*:** Lets you specify host name or IP address of the TCP XML or TCP client provider.

  Example of a host name: OurDevice
  Example of an IP address: 123.123.123.123

- ***Port*:** Lets you specify the port number on which communication with the TCP XML or TCP client source takes place.

Managing Configurations

You define and edit the configurations of sources from the *Sources* tab in the *Transact Administrator* window.

Creating a Configuration

Note: You do not need to create new configurations for sources that use the source provider *TCP XML Transact provider*. Simply use the built-in configuration *Analytics*.

To create a new configuration to a source, do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Sources* tab, click the *Add New...* button if you want to add a new source or the *Edit*... button to edit an existing source. Define or – if required – edit the settings of the source in question as described in Managing Sources on page 22.

   You are now ready to add your new configuration.

3. In the *Create/Edit Source* window's *Configuration* section, click the *Add New...* button.

4. In the *Create Configuration* window's *Name* field, type a name for the configuration.

   Tip: If required, the name may contain spaces and special characters, such as @, $, %, æ, etc.

5. Click the *Capture from Source* button to capture some sample transaction data on which to base your configuration. This will open the *Select Input Source* window.

6. In the *Select Input Source* window, select the required input source, then click the *Start* button to being capturing transaction data.

   Wait sufficiently long for at least one, but preferably more, transactions to complete, then click the *Stop* button.

   See How to Capture Transaction Data on page 31 for more information about capturing transaction data.

7. Click *OK* to return to the *Create Configuration* window, in which the captured transaction data will now appear in the *Raw data* field.

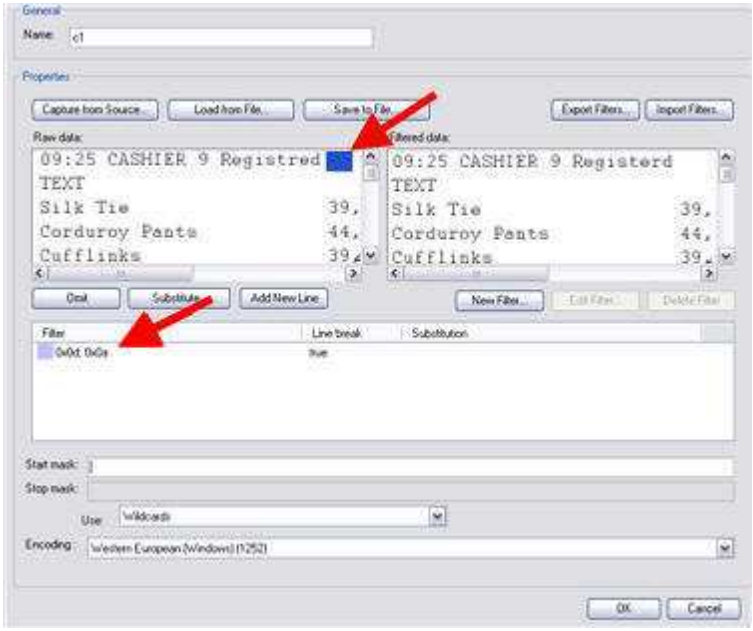
8. You are now ready to add filters: omit characters (i.e. define which characters to remove), add substitutions (i.e. define which characters to replace with other characters) and add line breaks.

   Note: The following is an example only. The example outlines the capture of a limited amount of raw (i.e. unformatted) transaction data, and how individual elements of the raw transaction data can subsequently be marked in order to be omitted, substituted, replaced with line breaks, indicate the beginning/end of a transaction, etc.

   In this example, we do the following:

   - We click and drag in the *Raw data* field to select two control characters (non-printing characters, typically used by printers for indicating line breaks, when to cut off a till receipt, etc.).

   - We click the *Add New Line...* button, and a line break is inserted instead of the two control characters. Furthermore, information about the two control characters replaced by the line break appear in the *[Filter overview list]*:



Also note how the *Filtered data* field changes accordingly. The *Filtered data* field provides a preview of how the transaction data will look when presented to end-users in the client applications.

In this example, the line break is all the formatting we require. In most cases, omissions (removal of certain content) and substitutions would be required as well. They are applied in a similar way, by dragging to select the required characters in the *Raw data* field, then clicking the relevant button. See How to Omit Characters on page 34, How to Use Substitutions on page 34 and How to Add Line Breaks on page 35 for more information.

9. When the required filters (omissions, substitutions or line breaks) are in place, add a start mask. The start mask defines when a new transaction begins, and thus helps keep individual transactions separate. See How to Use Start and Stop Masks on page 35 for more information.

   In this example, we do the following:

   - We have noticed that all new transactions begin with the characters *TEXT*. We therefore type *TEXT* in the *Start Mask* field. In the *Filtered data* field, Transact automatically inserts a horizontal line above occurrences of the start mask, as an indication of the beginning of a new transaction:

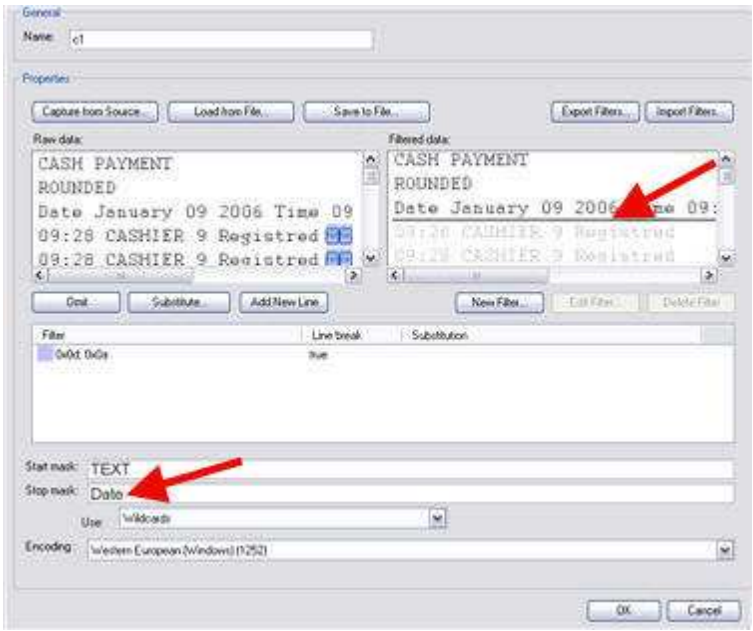
Note that start and stop masks are case sensitive; thus there is a difference between typing *TEXT* and *Text*.

10. Add a stop mask. The stop mask defines the end of a transaction.

Note: A stop mask is not compulsory, but can be useful if the received data contains irrelevant information—perhaps information about opening hours or special offers—between actual transactions.

In this example, we do the following:

- We have noticed that all transactions end with a line beginning with the characters *Date*. We therefore type *Date* in the *Stop Mask* field. In the *Filtered data* field, Transact automatically inserts a horizontal line below occurrences of the stop mask, as an indication of the end of a transaction:



In this example, the stop mask occurred at the beginning of a line, but start and stop masks may appear anywhere on a line: When Transact detects a start mask anywhere within a line, it will know that a new transaction begins with that line. When Transact detects a stop mask anywhere within a line, it will know that a transaction ends with that line.

Tip: You are able to use wildcards in start and stop masks. A wildcard is a special symbol that stands for one or more characters. Three different methods for wildcard use, selected in the *Use* field, are available. See The Create/Edit Configuration Window on page 36 for more information about the *Use* field and other configuration settings.

11. When ready, click OK to save the configuration.

Note: Configurations are saved together with the type of source (serial port, TCP client, TCP XML or Troy box) for which it has been created. However, exported filters can be used with configurations created for any type of source.

Tip: If you are going to create several near-identical configurations, you can use the *Copy...* button or the *Export Filters...* and *Import Filters...* buttons in the *Create/Edit Source* window to quickly create new configurations based on an existing configuration. See Copying a Configuration on page 32 and Exporting/Importing a Configuration on page 33 for more information.

How to Capture Transaction Data

You are able to capture sample transaction data on which to base your configuration. If relevant you can apply some filters and test your filters on the captured transaction data and see the result in the *Create/Edit Configuration* window while you are applying the filters.

To capture sample transaction data, do the following:

1. You access the *Select Input Source* window by clicking the *Capture from source...* button in the *Create/Edit Configuration* window.

2. In the *Select Input Source* window's (see page 39) top section, select the required input source.

   Tip: The list will only contain input sources matching the type of source you are currently working with. Example: If you are currently working with a configuration for a serial port source, only serial port input sources will appear in the list.

   Properties of the selected source will be displayed in the *Select Input Source* window's lower section.

3. Click the *Start* button to begin capturing transaction data.

   When clicked, the *Start* button changes to *Stop*.

4. Wait sufficiently long for at least one, but preferably more, transactions to complete.

   If the cash register, ATM, etc. providing the transaction data is visible from where you are situated, you will easily be able to determine how long to wait for. If the cash register, ATM, etc. is not visible, use the number of captured bytes (displayed near the bottom of the window after you click the *Start* button) as an indication of the amount of data captured. In most cases, capturing approximately 3000 bytes of data will suffice.

5. Click the *Stop* button to stop capturing transaction data.

6. When ready, click *OK.*

   The captured transaction data will now be displayed in the *Create/Edit Configuration* window's *Raw data* field, ready for use when defining the properties of the configuration..

Tip: You are able to save captured transaction data in a *.capture* file, and load the previously captured and saved transaction data when creating a new configuration. See The Create/Edit Configuration Window on page 36 for more information about the Load fro*m File...* and *Save to File...* buttons. See also Creating a Configuration on page 27 for more information about how to create a configuration.

Editing a Configuration

Note: You do not need to edit the built-in configuration *Analytics* that is used in connection with the source provider *TCP XML Transact provider*. Simply use the built-in configuration *Analytics* as is.

To edit a new configuration to a source, do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Sources* tab, click the *Add New...* button if you want to add a new source or the *Edit*... button to edit an existing source. Define or – if required – edit the settings of the source in question as described in Creating a Configuration on page 27.

3. In the *Create/Edit Source* window's *Configuration* section, click the *Edit...* button.

   You are now ready to edit the configuration. See How to Omit Characters on page 34, How to Use Substitutions on page 34, How to Add Line Breaks on page 35 and How to Use Start and Stop Masks on page 35 for more information about how to omit or substitute characters in the raw transaction data, how to add line breaks and define start and stop masks. See also The Create/Edit Configuration Window on page 36 for more information about all configuration settings.

   Tip: If you are going to create several near-identical configurations, you can use the *Copy...* button in the *Create/Edit Source* window to quickly create new configurations based on an existing configuration for the same type of source. You can also use the *Export Filters...* and *Import Filters...* buttons in the *Create/Edit Configuration* window to quickly create new configurations based on an existing configuration for a different type of source. See Copying a Configuration on page 32 and Exporting/Importing a Configuration on page 33 for more information.

   Note: Configurations are saved together with the type of source (serial port, TCP client, TCP XML or Troy box) for which it has been created. However, exported filters can be used with configurations created for any type of source.

Copying a Configuration

Note: You do not need to edit or copy the built-in configuration *Analytics* that is used in connection with the source provider *TCP XML Transact provider*. Simply use the built-in configuration *Analytics* as is.

You can copy configurations of the same source type (serial port, TCP client, TCP XML or Troy box) for easy reuse of existing configurations.

To copy a configuration, do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Sources* tab, click the *Add New...* button if you want to add a new source or the *Edit*... button to edit an existing source. Define or – if required – edit the settings of the source in question as described in Creating a Configuration on page 27 or Editing a Configuration on page 32.

3. In the *Create/Edit Source* window's *Configuration* section, select the required configuration and click the *Copy...* button.

   Note: Configurations are saved together with the type of source (serial port, TCP client, TCP XML or Troy box) for which it has been created. So if you have selected a serial port source, you can only select configurations defined for serial port sources. However, exported filters can be used with configurations created for any type of source.

4. Type a name for the configuration in the *Name* field and change the required settings. See The Create/Edit Configuration Window on page 36 for more information about the different configuration settings.

5. Click *OK* to save your new configuration.

Exporting/Importing a Configuration

If you want to reuse a configuration between different source types (serial port, TCP client or Troy box), you can export the configuration from one source type and import it when creating or editing the configuration for another source type.

Do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Sources* tab, select a source that has the required source type (serial port, TCP client or Troy box) for your export.

3. In the *Edit Source* window's *Configuration* section, select the required configuration and click the *Edit...* button.

4. In the *Edit Configuration* window, click the *Export Filters...* button.

5. Specify a name for the export file and save it by clicking *Save*. The exported configuration's filters are saved as a *.filter* file.

6. Click *Cancel* to close the *Edit Configuration* window.

7. Click *Close* to close the *Edit Source* window.

8. On the *Transact Administrator* window's *Sources* tab, select the source that should reuse the exported configuration settings and click the *Edit*... button.

   If you would like to add a new source, click the *Add New...* button. See Creating a Configuration on page 27 for more information.

9. In the *Create/Edit Source* window's *Configuration* section, click the *Add New...* or *Edit...* button as required.

10. In the *Create/Edit Configuration* window, click the *Import Filters...* button. Select your previously exported file and click *Open*.

11. Edit if relevant the imported filter settings. Specify a start mask and—if relevant—a stop mask and click *OK* to save your new configuration.

Tip: If you are going to create several near-identical configurations for several sources of the same source type, you can use the *Copy...* button in the *Create/Edit Source* window. See Copying a Configuration on page 32 for more information.

How to Omit Characters

You are able to filter out unwanted information (single or several characters) in the raw, unformatted transaction data.

To omit characters in a source's configuration, do the following:

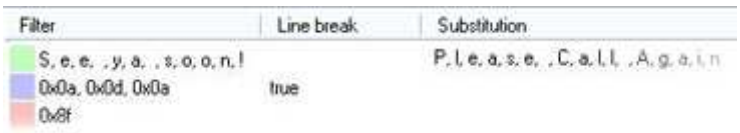
- In the *Create/Edit Configuration* window click and drag to select the characters in the *Raw data* field that you want to filter out.
- Click the *Omit* button to filter out (i.e. remove) the selected characters.

You can immediately view the effect of your filter in the *Filtered data* field.

Tip: You are able to omit regular characters as well as control characters. Control characters are non-printing characters, typically used by printers for indicating line breaks, when to cut off a till receipt, etc. Example of a control character as it appears when displayed in the *Raw data* field:

In the *Raw data* field, the selected characters will be highlighted in a light pink color:

The filtered out characters will furthermore be listed and highlighted in a light pink color in the *[Filters overview field]*.



Example of a substitution, a line break and an omission listed in the *[Filters overview field]*. In this example the control character *0x8f* has been filtered out completely.

Tip: If you are not happy with an applied filter, you can always remove or edit it: Select the unwanted filter in the *[Filters overview field]*, then click the *Delete Filter* or *Edit Filter...* button.

How to Use Substitutions

You are able to substitute information (one or more characters) in the raw, unformatted transaction data and replace it with new text or characters.

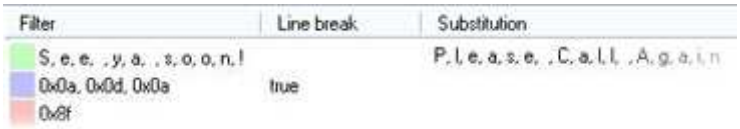
To substitute content in a source's configuration, do the following:

- In the *Create/Edit Configuration* window click and drag to select the characters in the *Raw data* field that you want to substitute.
- Click the *Substitute...* button to substitute (i.e. replace) the selected characters. In the *Edit Filter* window type the characters that you want replace the selected characters with in the *Substitution* field.

You can immediately view the effect of the substitution in the *Filtered data* field.

In the *Raw data* field, the selected characters will be highlighted in a light green color:

The characters to be substituted will furthermore be listed and highlighted in a light green color in the *[Filters overview field]*.



Example of a substitution, a line break and an omission listed in the *[Filters overview field]*. In this example, the characters forming *See ya soon!* have been substituted with *Please Call Again.*

Tip: You are able to substitute regular characters as well as control characters. Note, however, that new control characters must be specified in Hex notation, e.g. \x[0-F][0-F].

Tip: If you are not happy with an applied substitution, you can always remove or edit it: Select the unwanted substitution in the *[Filters overview field]*, then click the *Delete Filter* or *Edit Filter...* button.

How to Add Line Breaks

You are able to replace one or more characters, including control characters, with a line break so the initially received transaction data which typically consists of a single long string of information, can be presented in more reader-friendly manner.

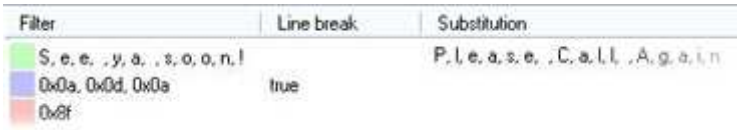
To add a line break, do the following:

- In the *Create/Edit Configuration* window click and drag to select the characters in the *Raw data* field that you want to substitute with a line break.
- Click the *Add New Line...* button.

You can immediately view the effect of the new line break in the *Filtered data* field.

In the *Raw data* field, the selected characters will be highlighted in a light purple color:

The characters to be replaced with a line break will furthermore be listed and highlighted in a light purple color in the *[Filters overview field]*.



Example of a substitution, a line break and an omission listed in the *[Filters overview field]*. In this example the control characters *0x0a0x0d0x0*a have been transformed into a line break.

Tip: If you are not happy with the applied line break, you can always remove or edit it: Select the unwanted line break in the *[Filters overview field]*, then click the *Delete Filter* or *Edit Filter...* button.

How to Use Start and Stop Masks

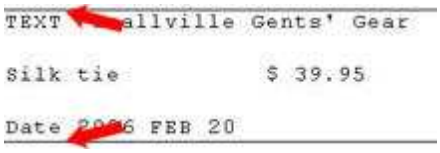
You are able to define a start and stop mask to indicate where a transaction ends and a new begins. Horizontal lines are inserted in the *Filtered data* field to visualize where the transaction starts and ends, and will thus help to keep individual transactions separate. A stop mask is not

compulsory, but can be useful if the received data contains irrelevant information—perhaps information about opening hours or special offers—between actual transactions.

To add a start or stop mask, do the following:

1. Open the *Transact Administrator* window.
2. On the *Transact Administrator* window's *Sources* tab, click the *Add New...* button if you want to add a new source or the *Edit*... button to edit an existing source.
3. In the *Create/Edit Source* window's *Configuration* section, click the *Add New...* or *Edit...* button depending on whether you want to add or edit a new configuration.
4. In the *Raw data* field in the *Create/Edit Configuration* window find the characters in the transaction data that indicates that a transaction begins or ends.
5. Type the start mask in the *Start mask* field and the stop mask in the *Stop mask* field.

In the *Filtered data* field, the start and stop mask will be indicated by a horizontal line:



This example shows a horizontal line inserted before the start mask *TEXT* and after the stop mask *Date*.

Tip: You are able to use wild cards in start and stop masks. Start and stop masks are case sensitive – unless using regular expressions. See the description of the *Use* field in The Create/Edit Configuration Window on page 36 for more information.

The Create/Edit Configuration Window

Configurations are managed in the *Transact* Administrator window's *Sources* tab since configurations are associated with and—customized to—the different sources.

You access the two main configuration windows *Create Configuration* or *Edit Configuration* by clicking the *Add New...* button in the *Create Source* window or *Edit Source* window.

The *Create/Edit Configuration* window has the following content:

- ***Name*:** Lets you specify a name for the configuration.

  Tip: If required, the name may contain spaces and special characters, such as @, $, %, æ, etc.

  Note: If your are creating/editing a configuration for the source provider *TCP XML Transact provider*, the *Name* setting is the only available setting in the *Create/Edit Configuration* window, since no configuration is needed for this source provider.

- ***Capture from Source...*:** Opens the *Select Input Source* window (see page 39), with which you are able to capture sample transaction data for use when creating the configuration. See How to Capture Transaction Data on page 31 for more information.

- ***Load from File...*:** Lets you load previously captured transaction data saved in a *.capture* file, and use the transaction data when creating the configuration.

- ***Save to File...*:** Lets you save any captured transaction data currently open in the *Create Configuration* window as a *.capture* file.

- ***Export Filters...*:** Lets you save the configuration's filters (omissions, substitutions or line breaks) as a *.filte*r file, which can subsequently be imported and used in other configurations. See Exporting/Importing a Configuration on page 33 for more information.

- ***Import Filters...*:** Lets you import previously exported *.filter* files.

- ***Raw data*:** Displays the raw transaction data, with indications of any added filters (omissions, substitutions or line breaks).

- ***Filtered data*:** Provides a preview of the transaction data as it will be presented in client applications when viewed by end-users, with the omissions, substitutions, line breaks and masks applied.

- ***Omit*:** Lets you filter out one or more characters selected in the *Raw data* field. See How to Omit Characters on page 34 for more information.

- ***Substitute...*:** Opens the *Edit Filter* window (see page 38), with which you are able to substitute one or more characters selected in the Raw data field. See How to Use Substitutions on page 34 for more information.

- ***Add New Line*:** Lets you replace one or more characters, including control characters, selected in the *Raw data* field with a line break. See How to Add Line Breaks on page 35 for more information.

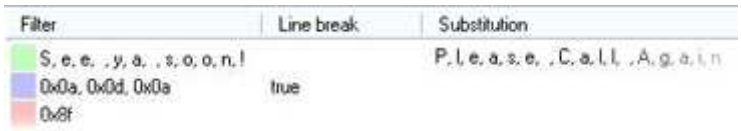
- ***New Filter...*:** Opens the *Edit Filter* window (see page 38), with which you are able to create filters (omissions, substitutions or line breaks) by typing the required characters rather than by selecting them in the Raw data field. See How to Omit Characters on page 34, How to Use Substitutions on page 34 and How to Add Line Breaks on page 35 for more information.

- ***Edit Filter...*:** Opens the *Edit Filter* window, with which you are able to edit the filter you have selected in the *[Filters overview field]*.

- ***Delete Filter*:** Lets you delete an existing filter selected in the *[Filters overview field]*.

- ***[Filters overview field]*:** Lists existing filters (omissions, substitutions or line breaks).

  Defined filters are highlighted with different colors. Unwanted content is indicated by a light pink color, substitutions by a light green color, and line breaks by a light purple color.



Example of a substitution, a line break and an omission listed in the *[Filters overview field]*.

- ***Start mask*:** Lets you define a start mask, i.e. which characters in the transaction data you want to be used for indicating the beginning of a new transaction. See How to Use Start and Stop Masks on page 35 for more information.

- ***Stop mask*:** Lets you define a stop mask, i.e. which characters in the transaction data you want to be used for indicating the end of a transaction.

- ***Use*:** You are able to use wildcards in start and stop masks. A wildcard is a special symbol that stands for one or more characters. Wildcards thus allow you to define start and stop masks without being 100% specific about the masks' character content.

  Two different types of wildcard use are available:

  - ***Wildcards*:** The start and/or stop mask are case sensitive. The following wildcards can be used: ? (any one or more characters or digits), * (zero or more characters or digits).

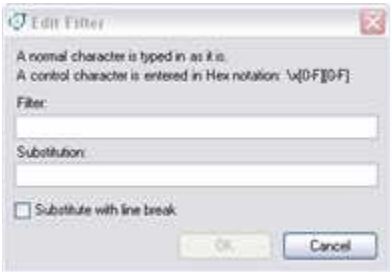
  - ***Regular Expression*:** Use regular expressions; a highly flexible method with which software developers and other people with programming knowledge are able to express how software should look for a text pattern, and what to do when the text pattern is found. Any case sensitivity, wildcards, etc. will depend entirely upon the way regular transactions are used in your environment.

- ***Encoding*:** Lets you select required character set to convert the source's transaction data which is sent in bites to understandable text in your language.

The Edit Filter Window

In the *Edit Filter* window you are able to create or edit filters (omissions, substitutions or line breaks). You can create new filters by clicking the *New Filter...* button and typing the required characters rather than by selecting them in the *Raw data* field. To edit an existing filter, select the required filter in the *[Filters overview field]* and click the *Edit Filter...* button.

The *Edit filter* window contains the following settings:



The Edit Filter window

- ***Filter*:** Field may be used for three purposes:

  - *If creating/editing an omission*: Type or edit the characters to be filtered out.

  - *If creating/editing a substitution*: Type or edit the characters to be substituted; then type/edit the characters you want to be used instead in the *Substitution* field.

  - *If creating/editing a line break*: Type or edit the characters to be replaced by a line break, then select the *Substitute with line break* check box.

- ***Substitution*:** Type or edit the characters to be used as substitution. The field is unavailable if the *Substitute with line break* check box is selected.

- ***Substitute with line break*:** Select if content of *Filter* field should be replaced by a line break. When this check box is selected any content in the *Substitution* field will be cleared.

See also How to Omit Characters on page 34, How to Use Substitutions on page 34 and How to Add Line Breaks on page 35 for more information about filters.

The Select Input Source Window

In the *Select Input Source* window you are able to capture sample transaction data for use when creating a configuration. You access the *Select Input Source* window by clicking the *Capture from Source...* button in the *Create/Edit Configuration* window. See How to Capture Transaction Data on page 31 for a step-by-step guide.

The *Select Input Source* window contains the following settings:

- ***Select a source for input sampling*:** Select the required input source from the list. The list will only contain input sources matching the type of source you are currently working with. Example: If you are currently working with a configuration for a serial port source, only serial port input sources will appear in the list.
- ***Properties*:** Names and values of the selected source are listed here.
- ***Start/Stop*:** Click the button to start or stop the capturing of transaction data.

The *Select Input Source* window; in this case only a single source is available for selection

Master/Slave Setup

You can set up several Milestone XProtect Transact servers in a master/slave relationship. The *Transact Administrator* window lets you define which servers you require as masters for the Transact server you are configuring. This enables Smart Client users to view transaction data from more than one Transact server.

Note: Only the Smart Client is able to display transaction data from slaves; this is not possible in the *Viewer* application.

You can get full benefit of a Milestone XProtect Transact master/slave setup if you have Milestone XProtect Enterprise or Milestone XProtect Corporate. This enables you to combine digital video monitoring from several surveillance servers with transaction data from all your Transact servers. If you have Milestone XProtect Professional or Milestone XProtect Basis+, you are still able to see transaction data from all your Transact master/slave servers and combine it with video from the surveillance server in the Smart Client.

- **Prerequisites - Milestone XProtect Professional or Milestone XProtect Basis+**
  The Transact master server must be located on the same computer as the surveillance server.

- **Prerequisites - Enterprise Servers**
  The Transact master server must be located on the same computer as the Enterprise master server, and Transact slave servers must be located on the same computers as the Enterprise slave servers.
  The Enterprise master/slave setup is defined in the *ImageServer Administrator* window. For more information see the separate Enterprise documentation.

- **Prerequisites – Corporate**
  The Transact master server must be located on the same computer as the Corporate management server.
  See Integrating with Milestone XProtect Corporate on page 52 for more information.

Once Transact is installed and the master/slave relationship defined, the surveillance master server sends information to Smart Clients about how to connect to its Transact master and slave servers. Then Smart Clients and the Transact servers communicate directly with each other for fastest updates.

Note: If you change a Transact slave's server settings in Transact Administrator, you must ask the Smart Client users to log out and in of their Smart Clients to reload the slave's server settings so that the data feed to the Smart Clients can continue.

See Managing Master/Slave Setup on page 40 and Creating a View with Transactions in the Smart Client on page 59 for more information.

A Transact server can be slave of any number of Transact master servers. It is a good idea to define more masters so you have transaction data redundancy. If the primary Transact master server for some reason should need maintenance, you can continue monitoring transaction data through one of the other Transact master servers.

Managing Master/Slave Setup

You can set up several Milestone XProtect Transact servers in a master/slave relationship. This enables you to view data from several Transact servers in the Smart Client. See Master/Slave Setup on page 39 for more information.

You define the master servers for the Transact server you are configuring by clicking the *Masters* tab in the Transact Administrator window.

Defining a Master Server

Prerequisites: When defining a master server for the Transact server you are configuring, you need to enter the master server's server settings. Have information about the master server's server settings ready when defining the master/slave setup.

To define a master server, do the following:

1. On the Transact server that is going to be configured as slave, open the Transact Administrator.

2. Click the *Masters* tab, then the *Add New...* button.

3. Specify the administration service name, host name and port number of the master server, and click *OK.*

Editing a Master Server

Prerequisites: When editing a master server for the Transact server you are configuring, you need to enter the master server's server settings. Have information about the master server's server settings ready when editing the master/slave setup.

To edit a master server, do the following:

1. On the Transact server that is configured as slave, open the Transact Administrator and click the *Masters* tab
2. Select the master server you want to edit, then click the *Edit...* button.
3. Edit the required settings in the *Master Information* dialog.

Removing a Master Server

To remove a master server from the list of master servers on the *Masters* tab, select the unwanted master server in the list and click the *Delete* button.

Updating Slave Information

To send a slave server's server settings to its master servers, click the *Update* button on the *Masters* tab.

Tip: When you change a slave server's server settings information, it is immediately sent to the server's master servers. If a master server for some reason is not running when this happens, you are notified. When the master server is running again, you can click the *Update* button to resend the slave server's updated server settings to its masters.

Master Setup Dialog Elements

The *MasterInformation* window contains five fields:

- ***Administration service name*:** The administration service name of the master server.
- ***Host*:** The IP address or host name of the master server.

  Example of a host name: OurDevice
  Example of an IP address: 123.123.123.123

- ***Port*:** The port number of the master server.

Tip: You find all of the above information about the master server's server settings on the master's *Server Setting* tab in the Transact Administrator.

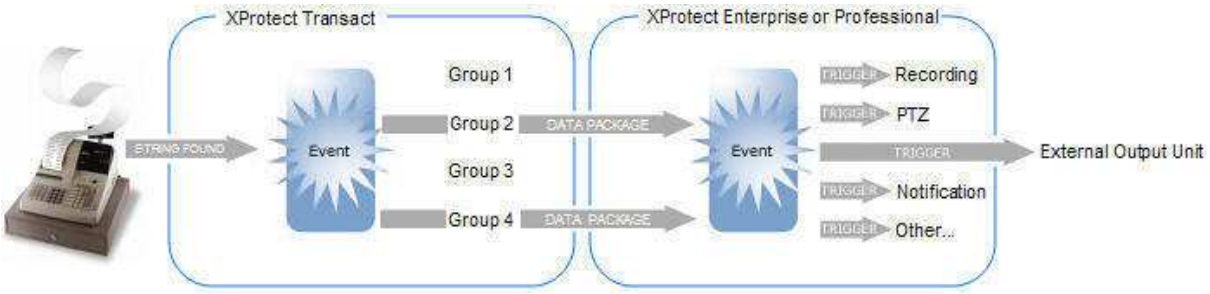
Events and Event Groups

Through Milestone XProtect Transact's event and event group features you are able to get Transact to listen for occurrences of specific words, numbers, characters etc. in the transaction data and generate events when the specified occurrences are found. When a occurrence is found an transaction event is triggered.

For easy and flexible usage of transaction events, you can group events in event groups. Each transaction event can be member of several groups. With event groups you also specify how transactions data is send to your surveillance system, and you can associate sources to an event group.

Note: Transaction events are supported in Milestone XProtect Enterprise and Milestone XProtect Professional. To trigger transactions events in the surveillance system it is prerequisite that you define generic events in the surveillance system that match the criteria of the transaction events from Transact.

When a transaction event is triggered, the transaction event groups containing the event send a TCP or UDP data package to Milestone XProtect Enterprise or Milestone XProtect Professional. The data package is then analyzed by the generic events in the surveillance system. If the transaction event is matching specified criteria in a generic event, the actions specified in the generic event are triggered.



Example: The source's transaction data contains an occurrence that triggers a transaction event. The transaction event is member of event groups 2 and 4. Each group sends a TCP or UDP data package to the surveillance system on which defined generic events triggers one or more actions.

See Managing Events on page 42, Managing Event Groups on page 44, How to Create a Generic Event Triggered by Transaction Data on page 45 , How to Test Events on page 47, Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 and Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

Managing Events

Through Milestone XProtect Transact's event and event group features you are able to get Transact to listen for occurrences of specific words, numbers, characters etc. in the transaction data and generate events when the specified occurrences are found. For easy and flexible usage of transaction events, you can group events in event groups. See Events and Event Groups on page 41 and Managing Event Groups on page 44 for more information.

You define and edit the events on the *Events* tab in the *Transact Administrator* window.

Adding an Event

To add an event, do the following:

1. Open the *Transact Administrator* window.
2. On the *Events* tab, click the *Add New...* button. This will open the *New Event* window.
3. In the *Name* field, specify a name for the new event.
4. In the *Search string* field, write the string you would like to search for in the transaction data. You can search for words, numbers and special characters that match the string you would like to find in the transaction data. You can only search for one string at a time. A string can however consist of several words or similar as long as this exactly matches the transaction data. You can for instance create a search string that listens for the occurrence of *Word1 Word2*. This will find occurrences of *Word1 Word2* but not occurrences of *Word2 Word1* or *Word1 Word3 Word2* etc.

Select *Case sensitive* if you would like to differentiate between upper and lowercase letters in the *Search string* field.

In the *Search type* field select between three ways of searching for the phrase specified in the *Search string* field:

- ***Simple*:** Use simple search, with which any transaction data containing an occurrence of the specified search string will be found.

- ***Exact*:** Use exact match, with which occurrences of the specified search string will be found only if they are preceded and followed by a blank space. Example: If you specify the search phrase *return*, only occurrences in which the phrase *return* appears surrounded by spaces will be highlighted, whereas occurrences such as *returned item* will not.

- ***Wildcards*:** Search using wildcards. Three different characters can be used as wildcards:

  The asterisk character (*). Place a asterisk after the search string, with which occurrences of the specified search string will be found also if the search string is followed by any number of characters. Example: If you specify *return** as your search string, all occurrences containing the letters *return*, such as *returned item, returns* and similar, will be highlighted.

  The question mark character (?), with which any single character can be substituted. Example: If you specify the search phrase *j?ck*, all occurrences such as *jack*, *jock*, etc. will be highlighted. You may use several question mark characters in your search. Examples: *jac???n* or *j?cks?n*.

  The hash character (#), with which any single digit can be substituted. Example: If you specify the search phrase *4#*, all occurrences such as *40*, *41*, etc. will be highlighted. You may use several hash characters in your search. Examples: *4##* or *12#4##7*.

5. In the *Event string* field specify the string that you want to send in a TCP/UDP data package to the surveillance system.

6. Click *OK* to save your settings.

When you have created an event, an event group and a generic event in your surveillance system that matches the criteria in the transaction event, you can test your transaction event to verify that the specified action is triggered in your surveillance system. See Managing Event Groups on page 44, How to Create a Generic Event Triggered by Transaction Data on page 45 , How to Test Events on page 47, Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 and Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

Editing an Event

To edit an event, do the following:

1. Open the *Transact Administrator* window.

2. On the *Transact Administrator* window's *Events* tab, select the required event and click the *Edit...* button. This will open the *Edit Event* window.

3. In the *Edit Event* window, change the required settings.

4. Click *OK* to save your settings.

Deleting an Event

To delete an event, select the required event on the *Transact Administrator* window's *Events* tab and then click the *Delete* button.

Managing Event Groups

For easy and flexible usage of transaction events, you can group events in event groups. Each transaction event can be member of several groups. With event groups you also specify how transactions data is send to your surveillance system, and you can associate sources to an event group. It is prerequisite that you define generic events in the surveillance system that match the criteria of the transaction events from Transact.

Note: Transaction events are supported in Milestone XProtect Enterprise and Milestone XProtect Professional.

See Sources and Configurations on page 20, Events and Event Groups on page 41 , Managing Events on page 42, How to Create a Generic Event Triggered by Transaction Data on page 45 , How to Test Events on page 47, Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 and Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

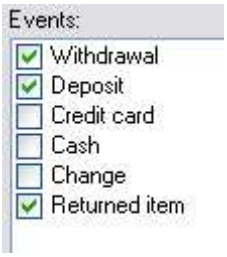
You define and edit the events groups on the *Event Groups* tab in the *Transact Administrator* window.

Adding an Event Group

To add an event group, do the following:

1. Open the *Transact Administrator* window.
2. On the *Event Groups* tab, click the *Add New...* button. This will open the *New Event Group* window.
3. In the *Name* field, specify a name for the new event group.
4. In the *Address* field, specify the host name or IP address of your surveillance system.
5. In the *Port* field, specify the port number on which to send events to your surveillance system. It is prerequisite that the specified port number is the same as the one the surveillance system uses when listening for generic events.

   Tip: The surveillance systems listen for generic events on the port specified as *Alert Port* in the surveillance system (default is port 1234). From the surveillance system's Administrator click the *Advanced...* button in the *I/O Setup* window to access the *Advanced* window to verify which port number is used.
6. In the *Protocol* field, specify whether you want to send the events as TCP or UDP data packages to the surveillance system. The default protocol is UDP since it uses less bandwidth than TCP. If your network does not support UDP, simply select TCP.
7. In the Events list you can see all events you have created. Select which events, you would like to include in the event group.



Example. Events with a checkmark are selected.

8. Click *OK* to save your settings.

   See How to Create a Generic Event Triggered by Transaction Data on page 45 for more information about how to create a generic event in your surveillance system that can be triggered by your new transaction event.

   When you have created an event, an event group and a generic event in your surveillance system that matches the criteria in the transaction event, you can test your transaction event to verify that the specified action is triggered in your surveillance system. See Managing Events on page 42, How to Create a Generic Event Triggered by Transaction Data on page 45, How to Test Events on page 47, Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 and Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

Editing an Event Group

To edit an event group, do the following:

1. Open the *Transact Administrator* window.
2. On the *Transact Administrator* window's *Event Groups* tab, select the required event group and click the *Edit...* button. This will open the *Edit Event Group* window.
3. In the *Edit Event Group* window, change the required settings.
4. Click *OK* to save your settings.

Deleting an Event Group

To delete an event, select the required event group on the *Transact Administrator* window's *Event Groups* tab, and then click the *Delete* button.

How to Create a Generic Event Triggered by Transaction Data

Generic events in Milestone XProtect Enterprise or Milestone XProtect Professional can be based on the analysis of received TCP and UDP data packets as it is the case with transaction events from Milestone XProtect Transact.

To add a generic event in Milestone XProtect Enterprise or Milestone XProtect Professional, do the following:

1. In the *Administrator* window, click the *Generic Events...* button.

   This will open the *Generic Events* window.

2. In the *Generic Events* window, first select the *Generic* item, then click the *Add new event...* button.

   This will open the *Add New Event* window in which you can specify the new event.

3. Now specify information in the following fields:

   - ***Event name*:** Specify a name for the event in the surveillance system. Note that event names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]

   - ***Event Protocol*:** Lets you select which protocol the surveillance system should listen for in order to detect the transaction event. Select the same protocol as the protocol specified for the transaction event that is to trigger this generic event. You can also select *Any* to be able to receive both TCP and UDP data packages.

   - ***Event rule type*:** Select how particular the surveillance system should be when analyzing received data packages: *Match* if the received package must contain only the exact message specified in the *Event message include* field (see description in the following), *Search* if the received package must contain the message specified in the *Event message include* field, but may also have other content.

   - ***Event priority*:** Specify a priority between 0 (lowest priority) and 1000 (highest priority) for the event, in case a received data package matches more than one event.

   - ***Event rule string*:** In the *Event substring* field, specify the Milestone XProtect Transact event string or parts of it that you want the surveillance system to listen for when analyzing the transaction data packages. Then click the *Add* button to add the specified term(s) to the *Event message include* field, the content of which is used when analyzing received data packages. You are furthermore able to use processing order parentheses and two different Boolean operators in the *Event message include* field by clicking the buttons to the right of the field.

     - (Optional) If requiring an e-mail alert to be sent automatically when the event occurs, select the *Send Email if this event occurs* check box. Note that in order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the surveillance system's *E-Mail setup* window.

     - (Optional) If requiring an SMS mobile phone text message alert to be sent automatically when the event occurs, select the *Send SMS if this event occurs* check box. Note that in order to be able to use SMS alerts, the SMS alert feature must have been set up in the surveillance system's *SMS settings* window.

4. When ready, click *OK.* This will return you to the *Generic Events* window. Click *OK* to close this window.

When you have created an event, an event group and a generic event in your surveillance system that matches the criteria in the transaction event, you can test your transaction event to verify that the specified action is triggered in your surveillance system. See Managing Events on page 42, Managing Event Groups on page 44, How to Test Events on page 47, Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 and Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

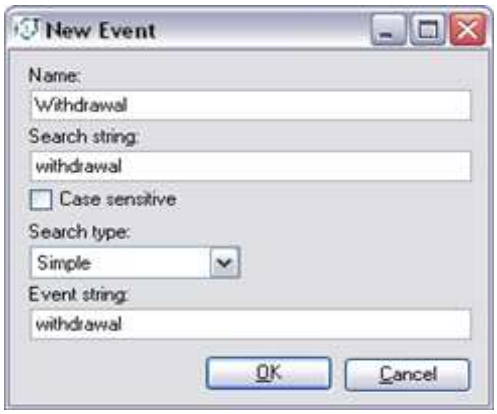
For more information about generic events see the separate documentation for Milestone XProtect Enterprise or Milestone XProtect Professional.

How to Test Events

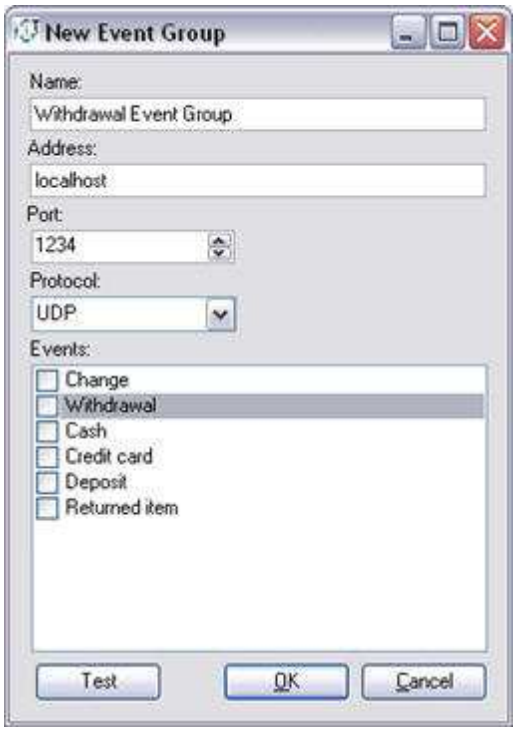
Once you have created a transaction event and added a generic event in your surveillance system that matches your transaction event, a quick and easy way to test your transaction event is to verify that an alert is generated in Smart Client.

In the example below we create a transaction event and a generic event in the surveillance system. Your required events may be different, but you can still use the principles outlined in the following:

1. Create an event called *Withdrawal*, that listens for occurrences of the string *withdrawal* and sends the event string *withdrawal* to the surveillance system. See Managing Events on page 42 for more information.



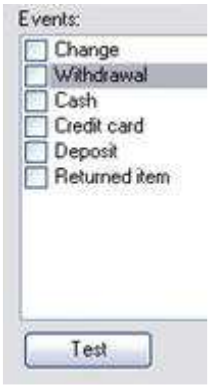
2. Create an event group called *Withdrawal Event Group* and fill in the necessary information about the surveillance systems address and port number. Select UDP as protocol. See Managing Event Groups on page 44 for more information.



3. Create a generic event called *Withdrawal* in your surveillance system's *Administrator* application. See How to Create a Generic Event Triggered by Transaction Data on page 45 for more information. Make sure that the selected protocol and event (rule) string matches the one in the *Withdrawal Event Group* created in step 2.

   Note: Access to features in the Administrator application, including generic events, may require administrator rights.

4. Now return to the *Transact Administrator* window, and from the *Event Groups* tab, select the event group *Withdrawal Event Group*. Select the *Withdrawal* event from the *Events* list and click the *Test* button.



Example: The event *Withdrawal* is selected for testing. You can also test events that are already included in the event group.

4. Open the Smart Client and log into the required surveillance server to verify that an alert matching your transaction event is generated on the *Browse* tab's *Alerts* section. See Viewing Alerts Triggered by Transaction Events in the Smart Client on page 49 for more information.

   Alternately open the *Viewer* to verify that an alarm matching your transaction event is present on the *Alarm Overview* control panel. See Viewing Alarms Triggered by Transaction Events in Viewer on page 50 for more information.

5. Till now you have only tested the transaction event. The event must be included in an event group and a source must be associated with the event group before Transact listens for occurrences in the transaction data. If the test was successful, include the *Withdrawal* event in the event group *Withdrawal Event Group*, and if required associate sources with the event group. See Managing Event Groups on page 44 and Managing Sources on page 22 for more information.

   If required you can include the event in other events groups. Repeat if relevant the test of the event in connection with the other events groups. If relevant select existing sources and associate them with event groups that include the *Withdrawal* event.

Viewing Alerts Triggered by Transaction Events in the Smart Client

If you have created a transaction event and added a generic event in your surveillance system that matches your transaction event, an alert is created in the Smart Client, each time the transaction event triggers an action in the surveillance system.

Do the following to see alerts triggered by transaction events in the Smart Client:

1. From the *Browse* tab's *Alerts* section, select the required alert from the *Alerts* list.

2. Click the *Get List* button.

   This will display a list of detected transaction events.

3. From the listed transaction events, click the required alert to view the transaction data and recordings from the selected alert in the view.

The transaction that is time-linked with the currently selected alert is highlighted with a yellow bar

Viewing Alerts Triggered by Transaction Events in Viewer

If you have created a transaction event and added a generic event in your surveillance system that matches your transaction event, an alarm is created in Viewer, each time the transaction event triggers an action in the surveillance system.

Do the following to see alarms triggered by transaction events in Viewer:

1. Click the *Alarm Overview* icon in Viewer's toolbar.

   This opens the *Alarm Overview* control panel.

2. In the *Alarm Overview* control panel, click the *Events* button.

   Now a list of alarms that originate from events is displayed.

3. From the listed transaction events, click the required alarm to view the transaction data and recordings from the selected event in the view.

The transaction that is time-linked with the currently selected alarm is highlighted with a yellow bar

Storage and Licensing Settings

On the *General Settings* tab in Transact Administrator you can define the default number of days to store transaction data and update your Transact installation's licensing information.

Default values
In this section you define the default duration for which to save transaction data.

- ***Default days to store transactions*:** Lets you specify the default number of days for which to store transaction data. If you do not specify otherwise, the default is seven days.

  Transaction data older than the specified number of days will be deleted from the Transact Database, and will therefore not be available for browsing in the client applications.

  Make sure the default number of days is sufficiently high to cover your organization's needs.

  Note: The field lets you specify a *default* number of days, which will be used if nothing else has been defined for individual sources. See *Adding a New Source* in the Managing Sources topic on page 22 for more information about how to define transaction storage periods for individual sources.

License
In this section you are able to see your Transact Administrator Software License Code (SLC) and update the Connection License Key (CLK).

Above the *Software License Code (SLC)* field you can see the MAC address of your computer. Below the *Connection License Key (CLK)* field you can see how many sources you are able to view simultaneously.

See About Licensing on page 14 for more information.

Client-side Preparations

With the Smart Client or *Viewer* application, you are able to view transaction data together with recordings of the transaction taking place.

When you want to browse transaction data and video recordings together, you open either the *S*mart Client or the *Viewer* application.

- The Smart Client requires that a plugin is installed; see Installing the Transact Plugin for the Smart Client on page 55.

  The Smart Client offers extremely feature-rich access to time-linked transaction data and video recordings, among other things view of live transactions, export and print of transaction data and video, and advanced search features. If you have a Corporate surveillance solution see Integrating with Milestone XProtect Corporate on page 52 for more information.

- The *Viewer* application comes with all XProtect surveillance solutions except Milestone XProtect Corporate.

  The *Viewer* offers basic access to time-linked transaction data and video recordings.

In the *S*mart Client or *Viewer* you simply create a view, select the required transaction data source (for example a particular cash register), then the required video sources (for example two cameras covering the area around the cash register from different angles), and you are ready to browse. See Creating a View with Transactions in the Smart Client on page 59 for more information.

The time-linking of the transaction data and video recordings enables you to view and browse the transaction data and video recordings simultaneously.

Browsing of transactions and video recordings in the *Viewer* and the *Smart Client* respectively

Integrating with Milestone XProtect Corporate

If your organization has Milestone XProtect Corporate surveillance solutions and you want to view transaction data together with recordings from cameras defined in a Milestone XProtect Corporate solution, you must add the Transact master server in the XProtect Corporate Manager application, before Transact and Corporate can communicate with each other.

Prerequisite: The Transact Server and the Corporate Management Server must be installed on the same computer.

Tip: If you have several Milestone XProtect Transact servers in a master/slave relationship, define the Transact Server that shares the computer with the Milestone XProtect Corporate

Management Server as master. See Managing Master/Slave Setup on page 40 for more information.

When the communication between the Transact Server and the Corporate Management Server is established, you will be able to view transaction data together with recordings from Corporate cameras in Smart Clients.

To add a Transact Server in the Corporate Manager application, do the following:

1. Open the Milestone XProtect Corporate Manager.
2. From the Corporate Manager's *Tools* menu, select *XProtect Enterprise Servers...*
3. In the *Add/Remove Protect Enterprise Servers* window, click the *Add...* button.

4. Enter the IP address or the host name of the required Transact server in the *XProtect Enterprise server IP / Host name* field.
5. Enter the port number used by the Transact server in the *Port number* field.

   Tip: The Transact server's default port number is 9001; if in doubt, you can find the port number used by the required Transact server on the Transact Administrator's *Server Settings* tab.

6. Enter your user name and password in the *Username* and *Password* fields. You can do this in two ways:

   - Select *Windows* and click the browse button to the right of the *Username* field to use the Windows authentication method which authenticates the administrator through the administrator's Windows login.

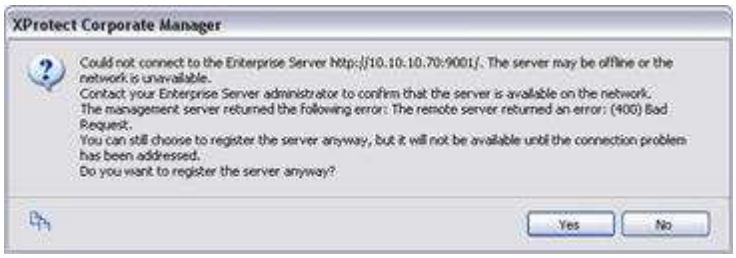
     - or -

   - Select *Basic* and enter the Milestone XProtect Enterprise administrator's user name and password in the *Username* and *Password* fields.

   Note: You must enter a user name, but the information is not used since access to transaction data is not restricted by user rights and Corporate roles.

7. Click *OK* to close the *Add XProtect Enterprise Server* window.

   The following error message is shown:


XProtect Corporate Manager
Could not connect to the Enterprise Server http://10.10.10.70:9001/. The server may be offline or the network is unavailable.
Contact your Enterprise Server administrator to confirm that the server is available on the network.
The management server returned the following error: The remote server returned an error: (400) Bad Request.
You can still choose to register the server anyway, but it will not be available until the connection problem has been addressed.
Do you want to register the server anyway?
Yes
No

8. Ignore the error message, and click *Yes* to add the Transact server.

   The Transact server is now listed in *Add/Remove Protect Enterprise Servers* window with the name *Unknown* and the status *Offline*.

9. Click the *Network...* button to define that Corporate will be handling the token authentication of the Smart Clients.

10. Specify the LAN IP address of the Milestone XProtect Corporate Management Server.

11. When you are ready, click *OK*.

12. Click *Close* to close the *Add/Remove Protect Enterprise Servers* window.

You are now ready to view transaction data together with recordings from Corporate cameras in Smart Clients. See Installing the Transact Plugin for the Smart Client on page 55 and Creating a View with Transactions in the Smart Client on page 59 for more information.

Installing the Transact Plugin for the Smart Client

Viewing of transactions in the Smart Client requires that a Transact Plugin is installed on the computer running the Smart Client.

Everyone using a Smart Client with Transact must download and install the plugin. Even if you are going to use the Smart Client on the same computer as the Transact Server, you should still download and install the plugin.

Depending on whether you want to view transaction data with video recordings from a Milestone XProtect Corporate surveillance solution or a Milestone XProtect Enterprise or Professional or Basis+ surveillance solution, the installation of the Smart Client Transact Plugin is different.

Installing with a Enterprise or Professional or Basis+ Solution

To download and install the Smart Client Transact Plugin, do the following:

1. Open an Internet Explorer browser (version 6.0 or later), and connect to the URL or IP address specified by your system administrator in order to connect to the surveillance system server.

   When you connect to the surveillance system server, you will see a welcome page.

2. In the *XProtect Smart Client* section of the welcome page, click the *Download and install plugins* link:

Welcome to Milestone Systems
XProtect
Remote Client & Smart Client
Please select:
XProtect Smart Client
• Download and install XProtect
• Download and install plugins
XProtect Remote Client
• Run XProtect Remote Client from server in full screen mode
• Run XProtect Remote Client from server in browser mode
• Download and install XProtect Remote Client locally
Remember my settings
milestone

3. In the *Transact 2.5 plugin for Smart Client* section, click the *Download and install plugin locally* link:

4. Depending on your security settings, you may receive a security warning (*Do you want to run or save this file?*). When this is the case, click the *Run* button.

5. Depending on your security settings, you may receive a further security warning (*Do you want to run this software?*). When this is the case, click the *Run* button.

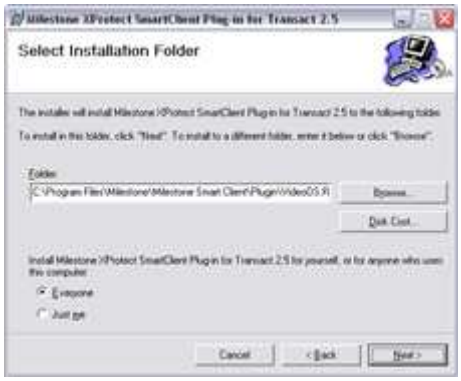
6. The *Milestone Smart Client Plugin for Transact 2.5* Setup Wizard opens:

Click *Next*.

7. Read the license agreement, and select *I Agree* to accept the license terms:

Then click *Next* to continue.

8. Select required installation folder (a default installation folder is automatically suggested). Also select who (just you or everyone) should be able to access the plugin (if in doubt, select *Everyone*):



Then click *Next*.

9. Click *Next* again to start the actual installation of the plugin:

10. When installation is complete, click the *Close* button:

See Creating a View with Transactions in the Smart Client on page 59 and the separate Milestone XProtect Transact User's manual for more information about how to view transaction data together with video recordings in your Smart Client.

Installing with a Corporate Solution

To download and install the Smart Client Transact Plugin, do the following:

1. Double-click the *TransactPluginInstaller.exe* file.

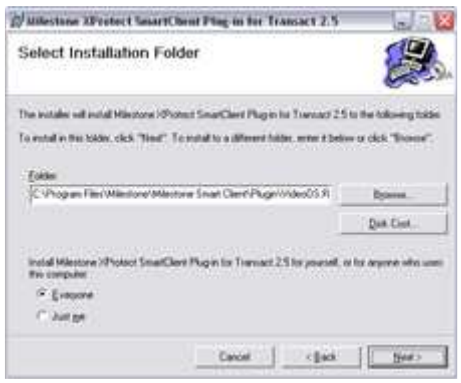
2. The *Milestone Smart Client Plugin for Transact 2.5* Setup Wizard opens:

   Click *Next*.

3. Read the license agreement, and select *I Agree* to accept the license terms:

   Then click *Next* to continue.

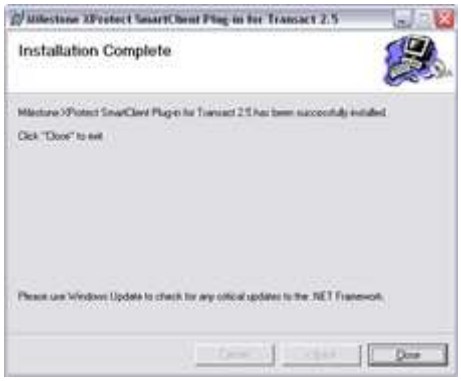
4. Select required installation folder (a default installation folder is automatically suggested). Also select who (just you or everyone) should be able to access the plugin (if in doubt, select *Everyone*):



Then click *Next*.

5. Click *Next* again to start the actual installation of the plugin:

6. When installation is complete, click the *Close* button:



See Creating a View with Transactions in the Smart Client on page 59 and the separate Milestone XProtect Transact User's manual for more information about how to view transaction data together with video recordings in your Smart Client.

Creating a View with Transactions in the Smart Client

If your Smart Client user rights permit you to create views, you are able to create views with transactions together with recordings. Simply create the required view with Transact content on the Smart Client's *Setup* tab.

Note: Creating a view may not be necessary if views in shared groups are used in your organization. Views in shared groups can be shared among Smart Client users. If a view with Transact content is available in a shared group, you may simply select the view on the Smart Client's *Live* or *Browse* tabs, and begin live viewing or browsing of transaction data with matching video recordings. Consult your system administrator if in doubt about whether views in shared groups are available in your organization.

To create a view with Transact content, do the following:

1. Open and log in to the Smart Client.

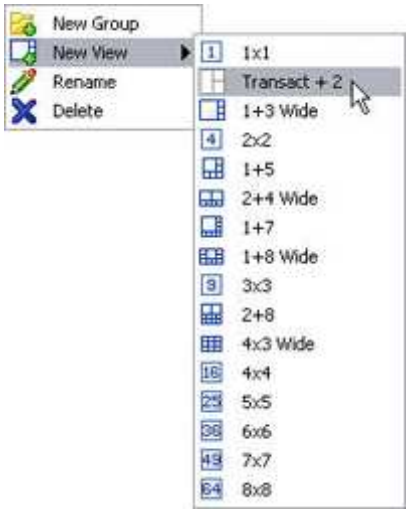
   Tip: For information about how to open and log in to the Smart Client, see separate

documentation for your Smart Client.

2. In the Smart Client, select the *Setup* tab.

3. On the *Setup* tab, create a new view.

   You may select any view layout from the list, but some layouts, such as the *Transact + 2* layout, are particularly suited for viewing transaction data and camera images together:



Example of available layouts; more layouts may be available in your version.

   Depending on requirements and user rights, you may create the view in a shared or private group.

   Tip: For further information about how to create views, see separate documentation for your Smart Client.

4. Drag the required cameras from the *Setup* tab's *System Overview* section to the view's camera slots.

5. This step may not be necessary if you are using one of the Transact views particularly suited for viewing transaction data and camera images together.

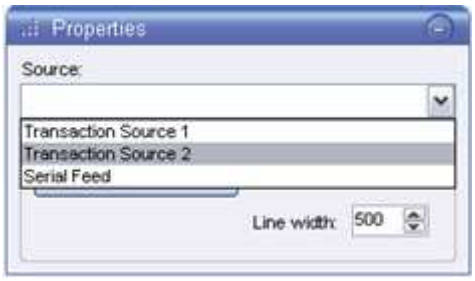
   Drag the *System Overview* section's *Transact Source* entry to the slot in which you want to view transaction data.

   The transaction data slot now changes color. However, you must still specify exactly which Transact source you want to view transaction data from.

Tip: If more than one Transact source is available, and if enough slots are available in the view, you can include more than one Transact source in the view. You can also create several views with different transaction sources.

See Status of Transaction Sources in the separate Milestone XProtect Transact User's manual for information about the status bar of transaction view slots and the different possible states of a source.

6. Select the view's transaction data slot, then expand the *Setup* tab's *Properties* section and select the required source:



Transaction data from the selected source is now displayed in the view:

Repeat if your view should contain more than one Transact source.

The view is now ready for use.

Tip: You are able to change the font size used for displaying the transaction data as well as the line width. You change these settings in the *Setup* tab's *Properties* section.

Removing the Software

You are able to remove your Transact installation in the following way:

Removing the Transact Software

To remove the Transact software, do the following:

1. On the computer on which the Transact software is installed, select *Start* > *Control Panel* > *Add or Remove Programs* to open the *Add or Remove Programs* window.

2. In the *Add or Remove Programs* window, select the *Milestone XProtect Transact 2.5* entry, and click the *Remove* button.

3. You will be asked to confirm that you want to remove Transact from the computer. If you are sure, click the *Yes* button and follow the remaining instructions.

Removing the Database

IMPORTANT: Removing the Transact Database will also remove all content of the database.

To remove the Transact Database, including all of its content, do the following:

1. On the computer on which the Transact software is installed, select *Start* > *Control Panel* > *Add or Remove Programs* to open the *Add or Remove Programs* window.

2. In the *Add or Remove Programs* window, select the *Microsoft SQL Server 2005* and click the *Remove* button.

3. In the *Microsoft SQL Server 2005 Uninstall* window select *VIDEOOS_TRANSACT:Database Engine* and click *Next*. If you can't select *VIDEOOS_TRANSACT:Database Engine* select *Remove SQL Server 2005 instance components* first.

4. You will be asked to confirm that you want to remove *Microsoft SQL Server 2005 (Database Engine: VIDEOOS_TRANSACT)* from the computer. If you are sure that you want to remove the database, click the *Finish* button and follow the remaining instructions.

Removing the Transact Plugin Installer

To remove the Transact Plugin Installer enabling users to download the Smart Client plugin (required for viewing transaction data in the Smart Client) from the Transact Server, do the following:

1. On the computer on which the Transact software is installed, select *Start* > *Control Panel* > *Add or Remove Programs* to open the *Add or Remove Programs* window.

2. In the A*dd or Remove Programs* window, select the *Milestone XProtect Transact Smart Client Plug-in Installer* entry, and click the *Remove* button.

3. You will be asked to confirm that you want to remove the plugin installer from the computer. If you are sure that you want to remove the plugin installer, click the *Yes* button and follow the remaining instructions.

Removing the Smart Client Plugin

To remove the Smart Client plugin required for viewing transaction data in the Smart Client, do the following:

1. On the computer on which the Smart Client plugin is installed, select *Start > Control Panel > Add or Remove Programs* to open the *Add or Remove Programs* window.

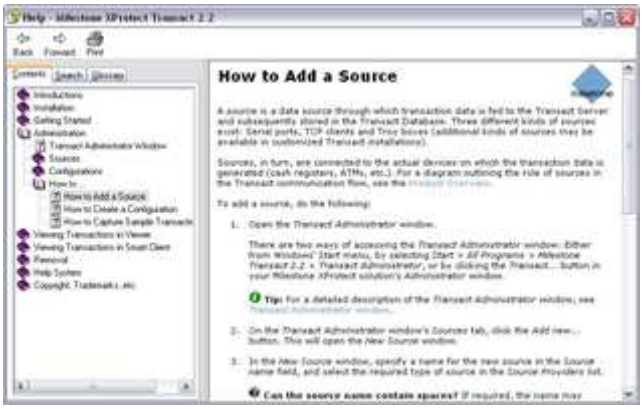
2. In the *Add or Remove Programs* window, select the *Milestone XProtect SmartClient Plug-in for Transact* entry, and click the *Remove* button.

3. You will be asked to confirm that you want to remove Milestone XProtect SmartClient Plugin for Transact from the computer. If you are sure that you want to remove the plugin, click the *Yes* button and follow the remaining instructions.

Using the Built-in Help System

To use Milestone XProtect Transact's built-in help system, simply press F1 on your keyboard.

When you press F1, the built-in help system will open in a separate window, allowing you to easily switch between help and the Transact administration windows.

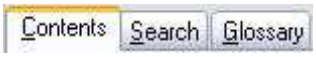


Example of Milestone XProtect Transact help window

The built-in help system is context sensitive. This means that when you press F1 for help while working in a particular Transact administration window, the help system automatically displays the help topic describing that window.

Navigating the Built-in Help System

Even though the help system initially takes you to a topic describing the window you are working in, you are always able to freely navigate between the help system's contents. To do this, simply use the help window's three tabs: Contents, Search and Glossary, or use the links inside the help topics.



Help system's three tabs

Contents Tab

The *Contents* tab lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer.

Search Tab

The *Search* tab lets you search for help topics containing particular terms of interest. For example, you can search for the term "server" and every help topic containing the term "server" will be listed in the search results. Clicking a help topic title in the search results list will open the required topic.

The *Search* tab contains a number of advanced search features; among these are the ability to quickly run previous searches, the ability to search topic titles only as well as the ability to display search results ranked according to presumed relevance.

Glossary Tab

What do abbreviations such as ATM, TCP or RS-232 stand for? The *Glossary* tab provides a glossary of common surveillance, transaction recording and network-related terms. Simply select a term to view a corresponding definition in the small window below the list of terms.

Three Types of Links in Help Topics

The actual content of each help topic is displayed in the right pane of the help window (i.e. the pane in which you are reading this text). Help topic texts may contain three types of links. Each type of link is described in the following:

Links to Related Topics

Clicking this type of link will take you to another topic within the help system.

Expanding Drop-Down Links

Clicking this type of link will display detailed information about a specific part of the help topic; for example a detailed description of a particular feature in one of Milestone XProtect Transact's windows. The detailed information is displayed immediately below the link itself; you are not taken to another page. Instead the content on the current page simply expands. Expanding drop-down links help save space; without them some detailed help topics would appear overly long and difficult to get an overview of.

Tip: If you wish to quickly collapse all texts from expanding drop-down links in a help topic, simply click the title of the topic in the help system's Contents menu.

Links to External Resources

Clicking this type of link will open an external resource in a separate browser window.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button:

When you click the *Print* button, a dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading. When this is the case, select *Print the selected topic* and click *OK*.

Tip: When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links (see *Three Types of Links in Help Topics* above), click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.

Glossary

A

ATM: Automatic Teller Machine; an unattended machine that dispenses cash when a personal coded card is used. ATMs are often placed outside banks.

AVI: A popular file format for video. Files in this format carry the .avi file extension.

C

CLK: Connection License Key; a registration key required for every transaction data source that can be viewed simultaneously on the surveillance system. If you do not have system administration responsibilities, you do not have to deal with CLKs. System administrators obtain CLKs as part of the software registration process. System administrators enter the CLK during installation and can update the CLK information in the Transact Administrator application.

Codec: A technology for compressing and decompressing audio and video data, for example in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

Configuration: 1) The way a software or hardware system is set up. 2) In this software specifically: Settings determining how received transaction data are transformed into presentable data, through the use of so-called filters and masks. This is necessary because the initially received transaction data typically consists of a single long string of information, in which it can be difficult to see when individual transactions begin and end.

Control Character: Non-printing characters; typically used by receipt printers for indicating line breaks, when to cut off a till receipt, etc.

D

DirectX: A Windows extension providing advanced multimedia capabilities.

DLK: Device License Key; a registration code required for every device (IP network camera or IP video server) installed on the surveillance system. If you do not have system administration responsibilities, you do not have to deal with DLKs. System administrators obtain DLKs as part of the software registration process. System administrators use the Import DLKs... feature in the Administrator application to import DLKs into the surveillance system.

Driver: A small program used for controlling / communicating with a device.

F

FPS: Frames Per Second, a measure indicating the amount of information contained in motion video. Each frame represents a still image, but when frames are displayed in succession the illusion of motion is created. The higher the FPS, the smoother the motion will appear. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame Rate: A measure indicating the amount of information contained in motion video. Typically measured in FPS (Frames Per second).

H

Host: A computer connected to a TCP/IP network. A host has its own IP address, but may - depending on network configuration - furthermore have a name (host name) in order to make it easily identifiable.

HTTP: HyperText Transfer Protocol, a standard for exchanging files across the internet. HTTP is the standard used for formatting and transmission of data on the world wide web.

I

I/O: Short for Input/Output.

IP: Internet Protocol; a protocol (i.e. standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP (Transmission Control Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

IP Address: Internet Protocol address; the identifier for a computer or device on a network. Used by the TCP/IP protocol for routing data traffic to the intended destination. An IP address consists of four numbers, each between 0 and 256, separated by full stops (example: 192.168.212.2).

IPIX: A technology that allows creation and viewing of 360-degree panoramic images. IPIX is a trademark of Internet Picture Corporation (IPIX).

M

MAC Address: Media Access Control address, a 12-character hexadecimal number uniquely identifying each device on a network.

MPEG: A group of compression standards and file formats for digital video developed by the Moving Pictures Experts Group (MPEG). MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information: Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reduce the size of MPEG files.

P

PoS: Point of Sale.

PTZ: Pan/Zoom/Tilt; a highly movable and flexible type of camera.

R

RS-232: Shot for Recommended Standard 232; a standard interface for connecting serial devices.

S

SLC: Software License Code; a product registration code required for using the surveillance system software. If you do not have system administration responsibilities, you do not have to deal with SLCs. System administrators use SLCs when installing and registering the software.

Source: A data source through which transaction data is fed to the server and onward to the client applications. Three different kinds of sources exist: Serial ports, TCP clients and Troy boxes. Sources, in turn, are connected to the actual devices on which the transaction data is generated (cash registers, ATMs, etc.).

T

TCP: Transmission Control Protocol; a protocol (i.e. standard) used for sending data packets across networks. IP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

Troy Box: Popular name for a Troy serial server.

V

Video Server: A device, typically a standalone device, which is able to stream video from a number of connected client cameras. Video servers contain image digitizers, making it possible to connect analog cameras to a network.

Headquarters (Denmark):

Milestone Systems A/S
Banemarksvej 50 G,
DK-2605 Brondby, Copenhagen, Denmark

Tel.: +45 88 300 300
Fax: +45 88 300 301

United Kingdom:

Milestone Systems UK Ltd.
118 Codnor Gate, Ripley
Derbyshire, DE5 9QW, England
Tel.: +44 (0) 1773 570 709

Italy:

Milestone Italia Srl.
Via Paisiello, 110
20092 Cinisello Balsamo
Milano, Italy
Tel.: +39 02 6179 7573-4
Fax: +39 02 6179 7531

Germany:

Milestone Systems DE
Am Kleefeld 6A
83527 Haag i. O.B., Germany
Tel.: +49 (0) 8072 442173

Japan:

Milestone Systems Japan
29-6, Sarugaku-cho, Shibuya-ku,
Tokyo 150-0033, Japan
Tel.: +81 (0) 3 3780 8749
Fax: +81 (0) 3 3476 4234
マイルストーン・システムズ
〒150-0033　東京都渋谷区猿楽町29 - 6 (デンマーク大使館内)

Singapore:

Milestone Systems Pte Ltd.
30 Robinson Road
13-03 Robinson Towers
Singapore 048456
Tel.: +65 6225 2686
Fax: +65 6225 1798

The Americas:

Milestone Systems Inc.
12725 SW Millikan Way, Suite 3
Beaverton, Oregon 97005, USA

Tel.: +1 503 906 7910 (see note)
Fax: +1 503 961 0221

If calling from the USA or Canada, phone tollfree 866-2-MILESTONE

www.milestonesys.com
info@milestonesys.com